Red Hat Enterprise Linux 4

Sicherheitshandbuch

Red Hat Enterprise Linux 4: Sicherheitshandbuch
Copyright © 2005 von Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Phone: +1 919 754 3700 Phone: 888 733 4281 Fax: +1 919 754 3701 PO Box 13588 Research Triangle Park NC 27709 USA

rhel-sg(DE)-4-Print-RHI (2004-09-30T17:12)
Copyright © 2005 Red Hat, Inc. Das vorliegende Material darf nur unter Einhaltung der in Open Publication License, V1.0 oder neuer dargelegten Geschäftsbedingungen vertrieben werden (die neueste Version ist gegenwärtig unter http://www.opencontent.org/openpub/ verfügbar).
Beträchtlich modifizierte Versionen dieses Dokumentes dürfen nur mit ausdrücklicher Genehmigung des Copyright-Inhabers vertrieben werden.
Der Vertrieb des Werks oder einer Ableitung des Werks in Standardbuchform (Papier) zu kommerziellen Zwecken ist nicht zulässig, sofern dies nicht zuvor durch den Copyright-Inhaber genehmigt wurde.
Red Hat und das Red Hat "Shadow Man" Logo sind eingetragene Warenzeichen oder Warenzeichen der Red Hat, Inc. in den USA und anderen Ländern.
Alle weiteren hier genannten Rechte an Warenzeichen sowie Copyrights liegen bei den jeweiligen Eigentümern.
Der GPG-Code des security@redhat.com Schlüssels lautet:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Inhaltsverzeichnis

Einführung ..... **i**
1. Architektur-spezifische Informationen ii
2. Dokumentkonventionen ii
3. Aktivieren Sie Ihr Abonnement v
3.1. Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein v
3.2. Geben Sie Ihre Abonnementnummer ein v
3.3. Verbinden Sie Ihr System vi
4. In der Planung vi
4.1. Senden Sie uns Ihr Feedback vi
I. Eine allgemeine Einleitung in Sicherheit ..... **i**
1. Überblick über Sicherheit 1
1.1. Was ist Computersicherheit? 1
1.2. Sicherheits-Kontrollen 6
1.3. Fazit 7
2. Angreifer und Schwachstellen 9
2.1. Ein kurzer geschichtlicher Überblick über Hacker 9
2.2. Bedrohungen der Netzwerksicherheit 10
2.3. Bedrohungen der Serversicherheit 10
2.4. Bedrohungen der Workstation- und Heim-PC-Sicherheit 12
II. Red Hat Enterprise Linux für Sicherheit konfigurieren **15**
3. Sicherheits-Updates 17
3.1. Pakete aktualisieren 17
4. Workstation-Sicherheit 23
4.1. Auswertung der Workstation-Sicherheit 23
4.2. BIOS und Bootloader Sicherheit 23
4.3. Passwortsicherheit 25
4.4. Administrative Kontrollen 31
4.5. Verfügbare Netzwerkdienste 36
4.6. Persönliche Firewalls 40
4.7. Kommunikationstools mit erhöhter Sicherheit 40
5. Server-Sicherheit 43
5.1. Sichern von Diensten mit TCP Wrappern und `xinetd` 43
5.2. Portmap sichern 46
5.3. Sichern von NIS 47
5.4. Sicherung von NFS 49
5.5. Sicherung des Apache HTTP Server 50
5.6. Sicherung von FTP 52
5.7. Sicherung von Sendmail 54
5.8. Bestätigen, welche Ports auf Verbindungen abhören 55
6. Virtuelle Private Netzwerke 57
6.1. VPNs und Red Hat Enterprise Linux 57
6.2. IPsec 57
6.3. Installation von IPsec 58
6.4. Konfiguration von IPsec Host-zu-Host 59
6.5. Konfiguration von IPsec Netzwerk-zu-Netzwerk 62
7. Firewalls 67
7.1. Netzfiler und `iptables` 68
7.2. Verwendung von `iptables` 69
7.3. Übliche `iptables` Filterung 70
7.4. `FORWARD` und NAT Regeln 71
7.5. Viren und geknackte IP-Adressen 73
7.6. `iptables` und dynamische Paketfilterung 74
7.7. `ip6tables` 74

7.8. Zusätzliche Informationsquellen ... 75
III. Sicherheit einschätzen ... 77
8. Schwachstellenanalyse ... 79
8.1. Denken wie der Feind ... 79
8.2. Definition von Analyse und Test ... 80
8.3. Auswerten der Tools ... 81
IV. Eindringung und Gegenmaßnahmen ... 85
9. Intrusion Detection ... 87
9.1. Definition der Intrusion Detection Systeme ... 87
9.2. Host-basiertes IDS ... 88
9.3. Netzwerk-basierte IDS ... 90
10. Vorfallsreaktion ... 93
10.1. Definition der Vorfallsreaktion ... 93
10.2. Erstellen eines Incident-Response-Plans ... 93
10.3. Implementieren des Incident-Response-Plans ... 95
10.4. Untersuchen des Vorfalls ... 95
10.5. Wiederherstellen von Ressourcen ... 98
10.6. Den Vorfall melden ... 99
V. Anhänge ... 101
A. Hardware- und Netzwerkschutz ... 103
A.1. Sichere Netzwerktopologien ... 103
A.2. Hardware-Sicherheit ... 106
B. Häufige Schwachstellen und Attacken ... 109
C. Häufige Ports ... 113
Stichwortverzeichnis ... 125
Colophon ... 131

Einführung

Willkommen beim *Red Hat Enterprise Linux Sicherheitshandbuch*!

Das *Red Hat Enterprise Linux Sicherheitshandbuch* wurde entworfen, um Benutzern von Red Hat Enterprise Linux beim Verständnis und Umgang mit der Sicherung von Arbeitsplatzrechnern und Servern gegen lokales und remotes Eindringen, Ausnutzung und böswillige Aktivitäten zu helfen. Das *Red Hat Enterprise Linux Sicherheitshandbuch* beschreibt im Detail die Planung und die Tools, die für die Errichtung einer sicheren Umgebung für Datenzentrum, Arbeitsplatz und Heimgebrauch benötigt werden. Durch Wissen, Wachsamkeit und Tools kann Red Hat Enterprise Linux zu einem voll funktionsfähigen und zugleich sicheren Betriebsystem werden, das vor allgemeinen Angriffen und Methoden des Datenraubs geschützt ist.

In diesem Handbuch werden verschiedene sicherheits-bezogene Themen im Detail beschrieben. Unter anderem:

- Firewalls
- Verschlüsselung
- Sicherheitskritische Services
- Virtuelle Private Netzwerke
- Intrusion Detection

Das Handbuch ist in folgende Teile unterteilt:

- Allgemeine Einführung in die Sicherheit
- Konfigurieren von Red Hat Enterprise Linux für Sicherheit
- Sicherheitsanalyse
- Einbrüche und Vorfallsreaktion
- Anhang

Wir möchten auf diesem Wege **Thomas Rude** für seine großzügigen Beiträge zu diesem Handbuch danken. Aus seiner Feder stammen die Kapitel *Anfälligkeits-Analyse* und *Vorfalls-Reaktion*. Danke Thomas!

In diesem Handbuch wird davon ausgegangen, dass Sie bereits über ein tiefgreifendes Wissen über Red Hat Enterprise Linux verfügen. Sind Sie noch neu oder verfügen über geringes bis mittelmäßiges Wissen über Red Hat Enterprise Linux und benötigen weitere Informationen über den Umgang mit diesem System, dann lesen Sie bitte folgende Handbücher, die die grundlegenden Aspekte von Red Hat Enterprise Linux näher beschreiben als das *Red Hat Enterprise Linux Sicherheitshandbuch*:

- *Red Hat Enterprise Linux Installationshandbuch* für Informationen zur Installation
- Das *Red Hat Enterprise Linux Einführung in die System-Administration* enthält einführende Informationen für neue Red Hat Enterprise Linux Systemadministratoren.
- Das *Red Hat Enterprise Linux Handbuch zur System-Administration* enthält weitere, detaillierte Informationen zur Konfiguration von Red Hat Enterprise Linux, abgestimmt auf Ihre Bedürfnisse als Anwender. Dieses Handbuch behandelt einige Services, die vom Sicherheitsstandpunkt aus auch im *Red Hat Enterprise Linux Sicherheitshandbuch* beschrieben werden.
- *Red Hat Enterprise Linux Referenzhandbuch* liefert detaillierte Informationen für erfahrenere Benutzer, auf die im Bedarf im Gegensatz zu einer Schritt-für-Schritt Anleitung zurückgegriffen werden können.

HTML-, PDF- und RPM-Versionen der Handbücher sind auf der Red Hat Enterprise Linux Dokumentations-CD und Online unter http://www.redhat.com/docs/ erhältlich.

Anmerkung

Obwohl dieses Handbuch die neuesten Informationen enthält, lesen Sie die *Red Hat Enterprise Linux Release-Notes* für weitere Information, die zum Druck dieses Handbuchs noch nicht vorlagen. Diese können auf der Red Hat Enterprise Linux CD #1 und Online unter http://www.redhat.com/docs/ gefunden werden.

1. Architektur-spezifische Informationen

Sofern nicht anders angegeben, bezieht sich jegliche Information in diesem Handbuch nur auf den x86-Prozessor und auf Prozessoren mit Intel® Extended Memory 64 Technology (Intel® EM64T) und AMD64 Technologien. Für Architektur-spezifische Informationen siehe das *Red Hat Enterprise Linux Installationshandbuch* für Ihre respektive Architektur.

2. Dokumentkonventionen

Beim Lesen dieses Handbuchs werden Sie feststellen, dass bestimmte Wörter in verschiedenen Fonts, Schriftbildern, Größen usw. dargestellt sind. Diese Unterscheidung folgt einer bestimmten Ordnung: bestimmte Wörter werden auf die gleiche Weise dargestellt, um darauf hinzuweisen, dass sie zu einer bestimmten Kategorie gehören. Typen von Begriffen, die auf diese Art dargestellt werden, schließen folgende Begriffe ein:

`Befehl`

Linux-Befehle (sowie Befehle anderer Betriebssysteme, sofern verwendet) werden auf diese Weise dargestellt. Diese Darstellungsart weist darauf hin, dass Sie das Wort oder den Satz in die Befehlszeile eingeben und die [Enter-Taste] drücken können, um den entsprechenden Befehl auszuführen. Gelegentlich enthält ein Befehl Wörter, die eigentlich auf eine andere Weise dargestellt werden würden (beispielsweise Dateinamen). In einem solchen Fall werden sie als Teil des Befehls betrachtet und der gesamte Satz wird als Befehl dargestellt. Beispiel:

Verwenden Sie den Befehl `cat testfile`, um den Inhalt einer Datei mit dem Namen `testfile` in einem aktuellen Verzeichnis anzeigen zu lassen.

`Dateiname`

Datei- und Verzeichnisnamen sowie die Namen von Pfaden und RPM-Paketen werden auf diese Weise dargestellt, was bedeutet, dass eine bestimmte Datei oder ein bestimmtes Verzeichnis mit diesem Namen in Ihrem System vorhanden ist. Beispiele:

Die Datei `.bashrc` in Ihrem Home-Verzeichnis enthält Bash-Shell Definitionen und Aliase für Ihren Gebrauch.

Die Datei `/etc/fstab` enthält Informationen über verschiedene Systemgeräte und Dateisysteme.

Installieren Sie den `webalizer` RPM, wenn Sie ein Analyseprogramm für eine Webserver-Protokolldatei verwenden möchten.

Applikation

Diese Darstellungsart weist darauf hin, dass es sich bei diesem Programm um eine Endbenutzer-Anwendung handelt (im Gegensatz zur System-Software). Beispiel:

Verwenden Sie **Mozilla**, um im Web zu browsen.

[Taste]

Die Tasten der Tastatur werden auf diese Weise dargestellt. Beispiel:

Um die [Tab]-Vervollständigung zu verwenden, geben Sie einen Buchstaben ein und drücken Sie anschließend die Taste [Tab]. Auf diese Weise wird die Liste der Dateien im Verzeichnis angezeigt, die mit diesem Buchstaben beginnen.

[Tasten]-[Kombination]

Eine Tastenkombination wird auf diese Art und Weise dargestellt.

Mit der Tastenkombination [Strg]-[Alt]-[Rücktaste] beenden Sie Ihre grafische Sitzung und kehren zum grafischen Anmeldebildschirm oder zur Konsole zurück.

Text in der GUI-Schnittstelle

Überschriften, Worte oder Sätze, die Sie auf dem GUI-Schnittstellenbildschirm oder in Window finden, werden in diesem Stil wiedergegeben. Wenn Sie daher einen Text in diesem Stil finden, soll dieser einen bestimmten GUI-Bildschirm oder ein Element eines GUI-Bildschirms (z.B. ein Text, der sich auf ein Kontrollkästchen oder auf ein Feld bezieht) identifizieren. Beispiel:

Wählen Sie das Kontrollkästchen **Passwort erforderlich**, wenn Ihr Bildschirmschoner passwortgeschützt sein soll.

Erste Menüstufe auf einem GUI-Bildschirm oder in einem Fenster

Wenn ein Wort auf diese Art und Weise dargestellt ist, zeigt dies an, dass es sich hierbei um den Anfang eines Pulldown-Menüs handelt. Beim Klicken auf das Wort auf dem GUI-Bildschirm erscheint der Rest des Menüs. Zum Beispiel:

Unter **Datei** auf dem GNOME-Terminal sehen Sie die Option **Neuer Tab**, mit dem Sie mehrere Shell Prompts im gleichen Fenster öffnen können.

Wenn Sie eine Befehlsreihe aus einem GUI-Menü eingeben wollen, wird diese entsprechend dem folgenden Beispiel angezeigt:

Indem Sie **Hauptmenü** (im Panel) => **Programmieren** => **Emacs** wählen, starten Sie den Texteditor **Emacs**.

Schaltfläche auf einem GUI-Bildschirm oder in einem Fenster

Diese Darstellungsweise zeigt an, dass man den betreffenden Text auf der Schaltfläche eines GUI-Bildschirms finden kann. Zum Beispiel:

Indem Sie auf die Schaltfläche **Zurück** klicken, kehren Sie auf die Website zurück, die Sie zuletzt angesehen haben.

`Computerausgabe`

Text, der in diesem Stil dargestellt wird, ist Text, der in einem Shell-Prompt ausgegeben wird, wie Fehlermeldungen und Antworten auf bestimmte Befehle. Zum Beispiel:

Durch Eingabe von `ls` erscheint der Inhalt eines Verzeichnisses. Zum Beispiel:

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

Die Ausgabe, die als Antwort auf den Befehl erscheint (in diesem Fall der Inhalt des Verzeichnisses), wird auf diese Art und Weise dargestellt.

`Prompt`

Ein Prompt wird auf diese Art und Weise dargestellt, wenn der Computer Ihnen mitteilen will, dass Sie nun eine Eingabe tätigen können. Beispiele:

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`Benutzereingabe`

Ein Text wird auf diese Art und Weise dargestellt, wenn er vom Benutzer entweder in die Befehlszeile oder in die Textbox auf einem GUI-Bildschirm eingegeben werden soll. Im folgenden Beispiel wird **`text`** in diesem Stil angezeigt:

Mit dem Befehl **`text`** am Prompt `boot:` booten Sie Ihr System in das textbasierte Installationsprogramm.

`replaceable`

Text, der für Beispiele benutzt wird und dafür vorgesehen ist, durch Daten ersetzt zu werden, wird in diesem Stil dargestellt. Im folgenden Beispiel ist <*`version-number`*> in dieser Form dargestellt.

Das Verzeichnis für den Kernel-Source ist `/usr/src/`<*`version-number`*>`/`, wobei <*`version-number`*> die Version des installierten Kernel ist.

Zusätzlich machen wir Sie mit Hilfe von bestimmten Strategien auf bestimmte Informationen aufmerksam. Entsprechend dem Wichtigkeitsgrad, das die jeweilige Information für Ihr System hat, sind diese Items entweder als Anmerkung, Hinweis oder Warnung gekennzeichnet. Zum Beispiel:

Anmerkung

Beachten Sie, dass Linux ein fallspezifisches System ist. In anderen Worten bedeutet dies, dass Rose nicht das gleiche ist wie ROSE und dies auch nicht das gleiche wie rOsE.

Tipp

Das Verzeichnis `/usr/share/doc/` enthält zusätzliche Dokumentationen für im System installierte Pakete.

Wichtig

Wenn Sie die DHCP Konfigurationsdatei bearbeiten, werden die Änderungen erst wirksam, wenn Sie den DHCP-Daemon neu gestartet haben.

Achtung

Führen Sie keine alltäglichen Aufgaben als root aus — verwenden Sie hierzu ausser für den Fall, dass Sie einen root-Account für Ihre Systemverwaltung benutzen, einen regulären Benutzeraccount.

Warnung

Seien Sie vorsichtig und entfernen Sie lediglich die notwendigen Red Hat Enterprise Linux Partitionen. Das Entfernen anderer Partitionen könnte zu Datenverlusten oder zur Korruption der Systemumgebung führen.

3. Aktivieren Sie Ihr Abonnement

Bevor Sie auf Service- und Softwarewartungs-Information sowie auch der Support-Dokumentation zugreifen können, welche in Ihrem Abonnement inkludiert ist, müssen Sie Ihr Abonnement aktivieren, indem Sie sich bei Red Hat registrieren. Die Registrierung setzt sich aus folgenden simplen Schritten zusammen:

- Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein
- Geben Sie Ihre Abonnementnummer ein
- Verbinden Sie Ihr System

Wenn Sie das erste mal Ihre Red Hat Enterprise Linux-Installation booten, werden Sie aufgefordert sich bei Red Hat mittels **Setup Agent** zu registrieren. Indem Sie einfach den Eingabeaufforderungen im **Setup Agent** folgen, können Sie sämtliche Registrierungsschritte vervollständigen und Ihr Abonnement aktivieren.

Wenn Sie die Registrierung mittels **Setup Agent** (Netzwerkzugang ist erforderlich) nicht durchführen können, so können Sie alternativ dazu auch den Red Hat Registrierungsprozess online unter http://www.redhat.com/register/ verwenden.

3.1. Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein

Sollten Sie kein bestehendes Red Hat Login besitzen, so können Sie Ihre Benutzerkennung und Passwort kreieren, sobald Sie dazu im **Setup Agent** aufgefordert werden oder auch online unter:

```
https://www.redhat.com/apps/activate/newlogin.html
```

Ein Red Hat Login ermöglicht Ihnen Zugang zu:

- Software Updates, Errata und Maintenance via Red Hat Network
- Red Hat Ressourcen auf 'Technischer Support'-Ebene, Dokumentation und Wissensdatenbank

Sollten Sie Ihr Red Hat Login vergessen haben, so können Sie nach Ihrem Red Hat Login auch online suchen:

```
https://rhn.redhat.com/help/forgot_password.pxt
```

3.2. Geben Sie Ihre Abonnementnummer ein

Ihre Abonnementnummer befindet sich im Paket mit Ihrer Bestellung. Sollte sich in Ihrem Paket keine Abonnementnummer befinden, so bedeutet dies, dass Ihr Abonnement für Sie bereits aktiviert worden ist und Sie diesen Schritt überspringen können.

Sie können Ihre Abonnementnummer eingeben, wenn Sie dazu im **Setup Agent** aufgefordert werden oder Sie besuchen http://www.redhat.com/register/.

3.3. Verbinden Sie Ihr System

Der Red Hat Network Registrierungs-Client hilft Ihnen bei Ihrer Systemverbindung, sodass Sie schlussendlich Updates erhalten und mit dem System-Management beginnen können.

1. Während der Registrierung im **Setup Agent** — Ticken Sie die Optionen **Hardware-Information senden** und **System-Paketliste senden**, sobald Sie dazu die Eingabeaufforderung erhalten.
2. Nachdem die Registrierung im **Setup Agent** abgeschlossen wurde — Vom **Hauptmenü** aus gehen Sie zu **System-Tools** und wählen dort **Red Hat Network** aus.
3. Nachdem die Registrierung im **Setup Agent** abgeschlossen wurde — Geben Sie folgenden Befehl von der Befehlszeile als root-Benutzer ein:
   - `/usr/bin/up2date --register`

4. In der Planung

Das *Red Hat Enterprise Linux Sicherheitshandbuch* ist Bestandteil von Red Hats wachsender Verantwortung, Red Hat Enterprise Linux Benutzern nützlichen und rechtzeitigen Support zu liefern. Mit dem Erscheinen neuer Tools und Sicherheitsmethodologien wird dieses Handbuch um diese erweitert.

4.1. Senden Sie uns Ihr Feedback

Wenn Sie einen Tippfehler im *Red Hat Enterprise Linux Sicherheitshandbuch* finden oder eine Idee haben, wie wir dieses Handbuch verbessern können, lassen Sie uns dies bitte wissen! Schreiben Sie an Bugzilla (http://bugzilla.redhat.com/bugzilla/) und geben Sie die Komponenten `rhel-sg` an.

Vergessen Sie dabei nicht, die Identifikationsnummer des Handbuchs anzugeben:

```
rhel-sg(DE)-4-Print-RHI (2004-09-30T17:12)
```

Durch Angeben dieser Handbuch-Identifikationsnummer wissen wir dann genau, welche Version des Handbuches Sie haben.

Wenn Sie einen Vorschlag zur Verbesserung der Dokumentation haben, sollten Sie uns hierzu möglichst genaue Angaben machen. Wenn Sie einen Fehler gefunden haben, geben Sie bitte die Nummer des entsprechenden Abschnitts und ein weinig vom Umgebungstext an, damit wir diesen leichter finden können.

I. Eine allgemeine Einleitung in Sicherheit

Dieser Abschnitt beschreibt Informationssicherheit, die Geschichte, und die Industrie, die daraus entstanden ist. Dieser Abschnitt schneidet auch einige Risiken an, auf die Computer-Benutzer und Administratoren stoßen.

Inhaltsverzeichnis

1. Überblick über Sicherheit 1
2. Angreifer und Schwachstellen 9

Kapitel 1.

Überblick über Sicherheit

Durch die wachsende Abhängigkeit von leistungsstarken, vernetzten Computern für das Führen von Unternehmen und Aufzeichnen unserer persönlichen Daten haben sich ganze Industriezweige um die Netzwerk- und Computersicherheit herum gebildet. Große Unternehmen haben das Wissen und die Fähigkeiten von Sicherheitsexperten zu Rate gezogen, um Systeme zu prüfen und maßgeschneiderte Lösungen für die Anforderungen des Unternehmens zu erstellen. Dadurch, dass die meisten Unternehmen dynamisch arbeiten, mit Mitarbeitern, die auf IT-Ressourcen der Firma intern und extern zugreifen, wird der Bedarf an sicheren Computing-Umgebungen immer deutlicher.

Leider betrachten viele Unternehmen (sowie auch Einzelbenutzer) die Sicherheit immer erst ganz zum Schluss, ein Prozess, der zu Gunsten erhöhter Leistung, Produktivität und Kostenfaktoren gerne übersehen wird. Angemessene Sicherheitsimplementierung wird oftmals *postmortem* durchgeführt — erst nachdem ein unberechtigter Zugriff erfolgte. Sicherheitsexperten sind sich einig, dass das Ergreifen richtiger Maßnahmen vor dem Verbinden mit einem unzuverlässigen Netzwerk wie dem Internet ein sicheres Mittel zum Verhindern von unerlaubten Zugriffen ist.

1.1. Was ist Computersicherheit?

Computersicherheit ist ein höchst allgemeiner Begriff, der einen weitreichenden Bereich an Computing und Informationsverarbeitung umfasst. Industriezweige, die von Computersystemen und Netzwerken hinsichtlich deren täglicher Geschäftstransaktionen und Zugriffe auf wichtige Daten abhängen, betrachten deren Daten als einen wichtigen Teil des Gesamtkapitals. Mehrere Begriffe und Metriken sind in unseren tagtägliches Geschäfts-Vokabular eingeflossen, wie zum Beispiel 'Total Cost of Ownership' (TOC) und 'Quality of Service' (QoS). Anhand dieser Metriken kalkulieren Unternehmen Aspekte wie Datenintegrität und Hochverfügbarkeit als Teil ihrer Planung. Das Erheben von Metriken ist ein anspruchsvoller Prozess im Projektmanagement. In einigen Industriezweigen wie zum Beispiel E-Commerce, ist die Verfügbarkeit und Verlässlichkeit von Daten der entscheidende Faktor zwischen Erfolg und Mißerfolg eines Unternehmens.

1.1.1. Wie entwickelte sich die Computersicherheit?

Viele Leser erinnern sich vielleicht an den Film "Wargames" mit Matthew Broderick in der Hauptrolle als High-School Schüler, der in den Supercomputer des US-Verteidigungsministeriums (DoD) einbricht und unabsichtlich fast einen Atomkrieg auslöst. In diesem Film verwendet Broderick sein Modem, um sich in den DoD-Computer (mit dem Namen WOPR) einzuwählen und mit der KI (Künstliche Intelligenz) Software, die sämtliche Atomwaffenlager steuert, Spiele zu spielen. Dieser Film wurde 1983 während des "Kalten Krieges" zwischen der ehemaligen Sowjetunion und den USA veröffentlicht und wurde als Erfolg gefeiert. Die Beliebtheit dieses Films inspirierte viele Individuen und Gruppen, einige der Methoden des jungen Protagonisten zum Einbruch in geheime Systeme zu implementieren, einschließlich des *war dialing* — eine Methode zum Suchen nach Telefonnummern für analoge Modemverbindungen in einem bestimmten Vorwahlbereich und einer Telefonvorwahlkombination.

Mehr als 10 Jahre später, nach einer 4-jährigen, mehrfachen gerichtlichen Verfolgung, bei der sogar das FBI (Federal Bureau of Investigation) und Computerexperten amerika-weit eingeschaltet wurden, wurde der Computer-Cracker Kevin Mitnick verhaftet und für 25 Straftaten durch Computerbetrug angeklagt. Es wurden durch ihn Schäden in der Höhe von über 80 Millionen US $ durch Verlust geistigen Eigentums sowie Quellcode von Nokia, NEC, Sun Microsystems, Novell, Fujitsu und Motorola verursacht. Zu dem Zeitpunkt sah das FBI hierin das größte computer-bezogene Verbrechen in der Geschichte der USA. Kevin Mitnick wurde für schuldig befunden und zu 68 Monaten Gefängnis

verurteilt, von denen er 60 Monate absaß, bevor er wegen guter Führung am 21. Januar 2000 entlassen wurde. Desweiteren durfte er keine Computer verwenden oder computer-bezogenes Consulting bis 2003 durchführen. Fahnder bestätigten, dass Mitnick ein Experte auf dem Gebiet des *Social Engineering* war — er missbrauchte soziale Kontakte, um Zugang zu Passwörtern und Systemen durch gefälschte Unterlagen zu erlangen.

Informationssicherheit hat sich in den letzten Jahren in Anbetracht der wachsenden Abhängigkeit von öffentlichen Netzwerken für persönliche, finanzielle und andere vertrauliche Informationen entwickelt. Die unzähligen Vorfälle, wie die Mitnick oder Vladimir Levin Fälle (weitere Informationen unter Abschnitt 1.1.2), haben Unternehmen aller Industriebereiche dazu veranlasst, deren Methoden zur Informationsübertragung und -Aufbewahrung neu zu überdenken. Die Beliebtheit des Internets war eine der wichtigsten Entwicklungen, die intensivere Bemühungen im Bereich der Datensicherheit mit sich brachte.

Eine immer größer werdende Anzahl von Anwendern verwendet deren persönliche Computer für den Zugriff auf Ressourcen, die das Internet zu bieten hat. Von simplen Nachforschungen und Recherchen bis hin zu E-Mail und Handelstransaktionen wird das Internet als eine der bedeutendsten Entwicklungen des 20. Jahrhunderts angesehen.

Das Internet und seine früheren Protokolle wurden jedoch als ein *trust-based* (auf Vertrauen basierendes) System entwickelt. Das heißt, dass das Internetprotokoll nicht von vornherein als sicher ausgelegt war. Es sind keine anerkannten Sicherheitsstandards im TCP/IP Kommunikations-Stack integriert, was eine Angriffsfläche für potentiell böswillige Benutzer und Prozesse im gesamten Netzwerk bildet. Moderne Entwicklungen haben die Kommunikation über das Internet sicherer gemacht, wobei es jedoch immer wieder zu Vorfälle kommt, die breites nationales Aufsehen erregen und uns bewusst machen, dass nichts hundertprozentig sicher ist.

1.1.2. Zeitleiste der Computer-Sicherheit

Verschiedene Schlüsselmomente trugen zur Geburt und zum Aufstieg von Computersicherheit bei. Im Folgenden werden einige, wichtige Ereignisse genannt, welche die Aufmerksamkeit auf Computer- und Informationssicherheit lenkten und zur deren heutiger Bedeutung beitrugen.

1.1.2.1. Die 30er und 40er Jahre

- Polnische Kryptografen (Entschlüssler) entwickeln 1918 die Enigma Maschine, eine elektro-mechanische Ziffern-Rotor-Anlage, welche reine Textnachrichten verschlüsselt. Ursprünglich entwickelt, um Kommunikation im Bankensektor abzusichern, wurde das Gerät von der Deutschen Streitmacht im Zweiten Weltkrieg zur sicheren Kommunikation eingesetzt. Ein brillianter Mathematiker namens Alan Turing entwickelt eine Methode, um die Verschlüsselungscodes von Enigma zu knacken, was den Alliierten wiederum ermöglichte Colossus zu entwickeln, eine Maschine, die wie so oft behauptet wird, dazu beigetragen hat, den Krieg ein Jahr früher zu beenden.

1.1.2.2. Die 60er Jahre

- Studenten am Massachusetts Institute of Technology (MIT) bilden den Tech Model Railroad Club (TMRC) und beginnen mit der Erforschung und Programmierung des PDP-1 Mainframe Computersystems dieser Universität. Durch diese Gruppe wurde eventuell auch der Begriff "Hacker" im heutzutage bekannten Kontext geprägt.
- Das US-Verteidigungsministerium bildet das Advanced Research Projects Agency Network (ARPANet), das in akademischen und Forschungs-Kreisen große Beliebtheit als Kanal für elektronischen Daten- und Informationsaustausch erlangt. Dies ebnet den Weg für die Erschaffung des Trägernetzwerks, das heute als das Internet bekannt ist.

- Ken Thompson entwickelt das UNIX Betriebssystem, weitverbreitet gepriesen als das "Hacker-freundlichste" Betriebssystem aufgrund der zugänglichen Entwicklungstools und Compilers und der hilfsbereiten Anwendergemeinschaft. Etwa zur gleichen Zeit entwickelt Dennis Ritchie die Programmiersprache C, die wohl beliebteste Hacker-Sprache in der Geschichte des Computers.

1.1.2.3. Die 70er Jahre

- Bolt, Berank und Newman, ein Vertragsunternehmen für Forschung und Entwicklung für die US-Regierung und Industrie, entwickelt das Telnet-Protokoll, eine öffentliche Erweiterung des ARPANets. Dies öffnete das Tor zur öffentlichen Verwendung von Datennetzwerken, einst beschränkt auf Vertragsunternehmen für die Regierung und akademische Forschung. Telnet ist jedoch, laut verschiedenen Sicherheitsexperten, das wohl unsicherste Protokoll für öffentliche Netzwerke.
- Steve Jobs und Steve Wozniak gründeten Apple Computer und begannen mit der Vermarktung des Personal Computer (PC). Der PC ist das Sprungbrett für böswillige Anwender zum Erlernen der Kunst, Systeme von außen mittels allgemein erhältlicher PC-Kommunikations-Hardware wie z.B. analoge Modems und War Dialers, zu cracken.
- Jim Ellis und Tom Truscott erschaffen USENET, ein Bulletin-Board-artiges System für elektronische Kommunikation zwischen ungleichen Anwendern. USENET wird schnell zu einem der beliebtesten Foren für den Ideenaustausch im Bereich Computing, Netzwerke und natürlich Cracking.

1.1.2.4. Die 80er Jahre

- IBM entwickelt und vertreibt PCs basierend auf dem Intel 8086 Mikroprozessor, einer relativ kostengünstigen Architektur, die elektronische Datenverarbeitung vom Büro ins traute Heim brachte. Dies half, den PC zu einem allgemeinen, zugänglichen Tool werden zu lassen, was wiederum zur Verbreitung dieser Hardware in den Haushalten und Büros böswilliger Anwender beitrug.
- Das Transmission Control Protocol (TCP), von Vint Cerf entwickelt, ist in zwei Teile unterteilt. Das Internet Protokoll (IP) wurde aus dieser Unterteilung geschaffen, und das TCP/IP Protokoll wird zum Standard jeglicher Kommunikation über das Internet.
- Basierend auf den Entwicklungen im Bereich des *Phreaking*, mit anderen Worten des Auskundschaften und Hacken von Telefonsystemen, wurde das Magazin *2600: The Hacker Quarterly* ins Leben gerufen und behandelt Themen wie das Hacken von Computern und Computer-Netzwerken für eine breite Leserschaft.
- Die 414-Gang (benannt nach der Vorwahlnummer des Wohnorts) wurde von den Behörden nach einer 9-Tage Cracking-Tour, bei der in Systeme von geheimen Orten wie das Los Alamos National Laboratory, einer Atomwaffen-Forschungseinrichtung, eingebrochen wurde, aufgegriffen.
- Die "Legion of Doom" und der "Chaos Computer Club" sind zwei Hacker-Gruppen, die mit der Erforschung von Anfälligkeiten in Computer- und Datennetzwerken beginnen.
- Der "Computer Fraud and Abuse Act" des Jahres 1986 (Gesetz gegen Computerbetrug und -missbrauch) wurde vom Kongress als Gesetz erlassen, basierend auf den Taten von Ian Murphy, auch bekannt als Captain Zap, der in Computer des Militärs einbrach, Informationen von Firmendatenbanken stahl und Anrufe über Telefonnummern der Regierung tätigte.
- Basierend auf dem "Computer Fraud und Abuse Act" war die Justiz in der Lage, den Studenten Robert Morris zu verurteilen, der den Morris Wurm auf über 6000 anfällige Computer im Internet verbreitet hatte. Der nächste bedeutende Fall im Rahmen dieses Gesetzes war Herbert Zinn, ein Schulabbrecher, der Systeme von AT&T und dem DoD gecrackt und missbraucht hatte.

- Basierend auf den Bedenken, dass der Morris-Wurm jederzeit repliziert werden könnte, wird das Computer Emergency Response Team (CERT) gegründet, um Benutzer von Computern vor Netzwerksicherheitsproblemen zu warnen.
- Clifford Stoll schreibt das Buch *The Cuckoo's Egg* (das Kuckucksei), eine Beschreibung der Untersuchung von Crackern, die unberechtigt auf sein System zugegriffen haben.

1.1.2.5. Die 90er Jahre

- ARPANet wird stillgelegt. Verkehr über dieses Netzwerk wir ans Internet weitergeleitet.
- Linus Torvalds entwickelt den Linux-Kernel für Verwendung mit dem GNU-Betriebssystem; die weitverbreitete Entwicklung und Verwendung von Linux liegt an der Zusammenarbeit der Benutzer und Entwickler, die über das Internet kommunizieren. Durch die Unix-Wurzeln ist Linux am beliebtesten bei Hackern und Administratoren, die Linux nützlich für das Erstellen von sicheren Alternativen zu Legacy-Servern mit proprietären (nicht-veröffentlichter Quellcode) Betriebssystemen fanden.
- Der grafische Web-Browser wird entwickelt und entflammt einen exponentiell höheren Bedarf an öffentlichem Internetzugang.
- Vladimir Levin und Komplizen knacken illegal die zentrale Datenbank der CitiBank und transferieren 10 Millionen US$ zu verschiedenen Konten. Levin wird von der Interpol verhaftet und fast die gesamte Summe sichergestellt.
- Unter Crackern wohl am meisten gefeiert ist Kevin Mitnick, der in verschiedene Systeme von Unternehmen einbrach und alles stahl, von persönlichen Informationen bekannter Persönlichkeiten bis zu mehr als 20 000 Kredikartennummern sowie Quellcode für proprietäre Software. Er wurde verhaftet, auf der Basis von Wire-Fraud angeklagt und verurteilt und verbrachte 5 Jahre in Haft.
- Kevin Poulsen und ein unbekannter Komplize manipulieren Telefonsysteme von Radiosendern, um bei Verlosungen Autos und Geldpreise zu gewinnen. Er wird wegen Computerbetrugs angeklagt und zu 5 Jahren Gefängnis verurteilt.
- Die Geschichten des Cracking und Phreaking werden zu Legenden und es treffen sich jährlich angehenden Cracker auf der DefCon-Versammlung, um das Cracken zu feiern und Ideen auszutauschen.
- Ein 19 Jahre alter israelischer Student wird verhaftet und als Organisator zahlreicher Einbrüche in Systeme der US-Regierung während des ersten Golfkrieges verurteilt. Angestellte des Militärs bezeichnen dies als den "am best-organisiertesten und systematischsten Angriff" auf Regierungssysteme in der Geschichte der USA.
- Die US-Generalbundesanwältin Janet Reno gründet als Antwort auf eskalierende Sicherheitsbrüche in Regierungssystemen das National Infrastructure Protection Center.
- Britische Kommunikationssatelliten werden von unbekannten Personen übernommen und Lösegeld gefordert. Die Britische Regierung gewinnt letzten Endes die Kontrolle über die Satelliten.

1.1.3. Sicherheit Heute

Im Februar 2000 wurde eine Distributed Denial of Service (DDoS) Attacke auf einige der am häufigsten besuchten Internetsites ausgeführt. Durch diese Attacke waren yahoo.com. cnn.com, fbi.gov und einige andere Sites für normale Benutzer unerreichbar, da Router mit stundenlangen riesigen ICMP-Paketübertragungen, auch *Ping Flood* genannt, überlastet waren. Diese Attacke wurde von unbekannten Angreifern gestartet, die speziell gefertigte, überall erhältliche Programme verwendeten, die verletzliche Netzwerkserver suchen und dann Client-Applikationen, auch *Trojaner* genannt, auf den Servern installieren und dann eine Attacke starten, bei der die Site des Opfers durch jeden

infizierten Server überflutet wird und somit unerreichbar wird. Viele schieben die Schuld auf fundamentale Fehler in der Weise, wie Router und Protokolle strukturiert sind, um alle eingehenden Daten anzunehmen, egal woher oder zu welchem Zweck Pakete gesendet wurden.

Dies bringt uns ins neue Jahrtausend, einer Zeit, in der geschätzte 945 Millionen Menschen weltweit das Internet verwenden oder verwendet haben (Computer Industry Almanac, 2004). Zur gleichen Zeit:

- Jeden Tag werden um die 225 schwerwiegenden Fälle von Sicherheitsverletzungen beim CERT Koordinationszentrum der Carnegie Mellon Universität (USA) gemeldet. [1]
- Im Jahre 2003 stieg die Anzahl der bei CERT gemeldeten Vorfälle sprunghaft von 82.094 im Jahre 2002 auf 137.529 an (52.658 im Jahre 2001). [2]
- Der weltweite wirtschaftliche Schaden, der durch die drei gefährlichsten Internetviren in den letzten zwei Jahren verursacht worden ist, wurde auf ungefähr 13,2 Billionen US-Dollar geschätzt. [Quelle: http://www.newsfactor.com/perl/story/16407.html]

Computersicherheit ist zu einer quantifizierbaren und berechtigten Ausgabe für alle IT-Budgets geworden. Unternehmen, die Datenintegrität und Hochverfügbarkeit benötigen, eruieren die Fähigkeiten von Systemadministratoren, Entwicklern und Ingenieuren, um eine 24/7 Verlässlichkeit ihrer Systeme, Services und Informationen zu garantieren. Opfer von böswilligen Anwendern, Prozessen oder koordinierten Attacken zu werden ist eine direkte Bedrohung in Hinsicht des Geschäftserfolges.

Leider kann System- und Netzwerksicherheit eine gewisse Schwierigkeit darstellen, die ein genaues Verständnis darüber, wie ein Unternehmen Informationen betrachtet, verwendet, manipuliert und überträgt erfordert. Das Verständnis darüber, auf welche Art ein Unternehmen (und dessen Mitarbeiter) Geschäfte betreibt, ist von höchster Bedeutung für die Einführung eines entsprechenden Sicherheitsplans.

1.1.4. Standardisierung von Sicherheit

Unternehmen in jedem Industriezweig sind auf Richtlinien und Regeln von Standardisierungsorganisationen wie z.B. der American Medical Association (AMA) oder dem Institute of Electrical and Electronics Engineers (IEEE) angewiesen. Die gleichen Ideale gelten für Informationssicherheit. Viele Sicherheitsberater und Hersteller haben sich auf das Standard-Sicherheitsmodell CIA, (*Confidentiality, Integrity und Availability*; Vertraulichkeit, Integrität und Verfügbarkeit) geeinigt. Dieses 3-Schichten Modell ist eine allgemein anerkannte Komponente für das Einschätzen von Risiken für vertrauliche Informationen und das Einrichten einer Sicherheitspolice. Im folgenden wird das CIA-Modell näher beschrieben:

- Vertraulichkeit — Vertrauliche Informationen dürfen nur für im vornherein festgelegte Einzelpersonen verfügbar sein. Unautorisierte Übertragung und Verwendung von Informationen muss eingeschränkt werden. So stellt zum Beispiel die Vertraulichkeit von Informationen sicher, dass persönliche oder finanzielle Details von Kunden nicht von Unbefugten für böswillige Zwecke wie Identitätsraub oder Kreditbetrug missbraucht werden kann.
- Integrität — Informationen dürfen nicht dahin gehend verändert werden, so dass sie unvollständig oder falsch werden. Unbefugte dürfen nicht in der Lage sein, vertrauliche Informationen ändern oder zerstören zu können.
- Verfügbarkeit — Informationen müssen jederzeit für befugte Personen zugänglich sein. Verfügbarkeit ist die Garantie dafür, dass Informationen mit einer vereinbarten Häufigkeit und rechtzeitig abgerufen werden können. Dies wird häufig in Prozent gemessen und formell in Service Level Vereinbarungen (SLAs), die von Netzwerkservice-Anbietern und deren Geschäftskunden verwendet werden, festgelegt.

1. Quelle: http://www.cert.org
2. Quelle: http://www.cert.org/stats/

1.2. Sicherheits-Kontrollen

Computersicherheit wird häufig in drei deutliche Hauptkategorien eingeteilt, die allgemein als *Kontrollen* bezeichnet werden:

- Zugangskontrolle
- Technische Kontrolle
- Administrative Kontrolle

Diese drei Kategorien definieren die Hauptziele einer ordnungsgemäßen Sicherheitsimplementierung. Innerhalb dieser Kontrollen befinden sich Unterkategorien, die deren Implementation tiefergehend beschreiben.

1.2.1. Zugangskontrollen

Die physikalische Zugangskontrolle ist die Implementierung von Sicherheitsmaßnahmen in einer festgelegten Struktur, die für die Verhinderung von unberechtigten Zugriffen auf empfindliche Informationen verwendet wird. Beispiele für physikalische Zugangskontrollen:

- Geschlossene Überwachungskameras
- Bewegungs- oder Wärmemelder
- Sicherheitspersonal
- Foto-IDs
- Verriegelte Stahltüren
- Biometrie (inkludiert Fingerabdruck, Stimmerkennung, Gesichtskontur, Irisscan, Handschrift und andere Methoden, um die Identität von Individuen nachzuweisen)

1.2.2. Technische Kontrollen

Technische Kontrollen verwenden Technologie als Basis für die Kontrolle von Zugang zu und Verwendung von empfindlichen Daten durch eine physikalische Struktur und über ein Netzwerk. Technische Kontrollen sind weitreichend in Umfang und umfassen unter anderem folgende Technologien:

- Verschlüsselung
- Smart Cards
- Netzwerkauthentifizierung
- Zugangskontrolllisten (ACLs)
- Dateiintegritäts-Prüfsoftware

1.2.3. Administrative Kontrollen

Administrative Kontrollen definieren den menschlichen Faktor der Sicherheit. Es umfasst alle Mitarbeiter innerhalb eines Unternehmens und legt fest, welche Anwender Zugang zu welchen Ressourcen und Informationen haben. Dies geschieht unter anderem durch:

- Training und Aufklärung
- Katastrophenvorbereitung und Wiederherstellungspläne
- Einstellungs- und Separationspläne

- Mitarbeiterregistrierung und Buchhaltung

1.3. Fazit

Nachdem Sie jetzt etwas über die Ursprünge, Beweggründe und Aspekte der Sicherheit gelernt haben, können Sie nun den richtigen Aktionsplan in Bezug auf Red Hat Enterprise Linux festlegen. Es ist wichtig zu wissen, welche Faktoren und Bedingungen die Sicherheit ausmachen, um eine richtige Strategie planen und implementieren zu können. Mit diesen Informationen im Hinterkopf kann der Prozess formalisiert werden, und der Weg wird klarer, je tiefer Sie in die Details des Sicherheitsprozesses eintauchen.

Kapitel 2.

Angreifer und Schwachstellen

Um eine gute Sicherheitsstrategie planen und implementieren zu können, müssen Sie als erstes einige der Wege, die entschlossene, motivierte Angreifer auskundschaften, um Systeme zu beeinträchtigen, verstehen. Bevor wir Ihnen jedoch diese im Detail beschreiben, geben wir Ihnen erstmal einen Überblick über die Terminologie, die zur Identifikation eines Angreifers verwendet wird.

2.1. Ein kurzer geschichtlicher Überblick über Hacker

Die moderne Bedeutung des Begriffs *Hacker* geht auf die 60er Jahre und den Massachusetts Institute of Technology (MIT) Tech Model Railroad Club zurück, der Modelleisenbahnen von großem Umfang und kleinstem Detail entwickelte. Als Hacker wurden Clubmitglieder bezeichnet, die einen Trick oder eine Lösung für ein Problem gefunden hatten.

Der Begriff Hacker wurde seit dem zur Beschreibung vieler verwendet, von Computerfreaks bis hin zu talentierten Programmierern. Was viele Hacker gemeinsam haben, ist das Verlangen, im Detail herauszufinden, wie Computersysteme und Netzwerke funktionieren, und das mit nur wenig oder ganz ohne Motivation von außen. Open Source Softwareentwickler betrachten sich selbst und ihre Kollegen oftmals als Hacker und verwenden das Wort als einen Respektsbegriff.

Typischerweise folgen Hacker einer Form von *Hacker-Ethik*, die vorgibt, dass die Suche nach Informationen und Wissen essentiell ist, und das das Teilen dieses Wissens eine Pflicht des Hackers gegenüber der Community ist. Während der Suche nach Wissen genießen einige Hacker die akademische Herausforderung, Sicherheitskontrollen für Computersysteme zu umgehen. Aus diesem Grund verwenden die Medien häufig den Begriff Hacker für jemanden, der unberechtigt mit skrupellosen, bösen oder kriminellen Absichten auf Systeme und Netzwerke zugreift. Ein zutreffenderer Begriff für diese Art von Computerhacker ist *Cracker* — ein Begriff, der Mitte der 80er Jahre von Hackern geschaffen wurde, um diese beiden Gruppen zu unterscheiden.

2.1.1. Graustufen

Es gibt einige wesentliche Unterschiede zwischen den einzelnen Personen, die Schwachstellen in Systemen und Netzwerken finden und ausbeuten. Diese Unterschiede werden durch die Farbe des Hutes, den sie "tragen" während sie ihre Sicherheitsforschungen durchführen, beschrieben, wobei die jeweilige Farbe synonym mit den jeweiligen Absichten ist.

Ein *White Hat Hacker* ist jemand, der Netzwerke und Systeme testet, um deren Leistung zu untersuchen und Anfälligkeiten auf Angriffe herauszufinden. Gewöhnlich cracken White Hat Hackers ihre eigenen Systeme oder die Systeme von Kunden, von denen sie zum Zwecke der Sicherheitsprüfung beauftragt wurden. Akademische Forscher und professionelle Sicherheitsberater sind zwei Beispiele für White Hat Hackers.

Ein *Black Hat Hacker* ist synonym mit einem Cracker. Im allgemeinen konzentrieren sich Cracker weniger auf das Programmieren und die akademische Seite des Einbruchs in Systeme. Sie verlassen sich häufig auf verfügbare Cracking-Programme und nutzen bekannte Schwachstellen in Systemen zur Aufdeckung empfindlicher Informationen aus, für persönlichen Gewinn oder um Schaden auf dem System oder Netzwerk anzurichten.

Ein *Grey Hat Hacker* auf der anderen Seite hat die Fähigkeiten und die Absichten eines White Hat Hackers in den meisten Fällen, nutzt sein Wissen von zeit zu Zeit jedoch auch für weniger edle Absichten. Ein Grey Hat Hacker kann also als jemand bezeichnet werden, der grundsätzlich gute Absichten hat, jedoch manchmal aus Eigennutz zum Black Hat Hacker wird.

Sogenannte "Grey Hat Hacker" halten sich häufig an eine andere Form von Hacker-Ethik, die besagt, dass es akzeptabel ist, in Systeme einzubrechen, solange der Hacker nicht Diebstahl begeht oder den Datenschutz verletzt. Man kann sich jedoch darüber streiten, ob das eigentliche Einbrechen in Systeme nicht bereits unethisch ist.

Unabhängig von der Absicht des Eindringlings ist es wichtig, die Schwachstellen zu kennen, die ein Cracker am ehesten versucht auszunutzen. Das restliche Kapitel behandelt diese Thematik.

2.2. Bedrohungen der Netzwerksicherheit

Unzureichende Methoden bei der Konfiguration einiger Netzwerkaspekte kann das Risiko eines Angriffs erheblich erhöhen.

2.2.1. Unsichere Architekturen

Ein fehlerhaft konfiguriertes Netzwerk ist der erste Zugangspunkt für unbefugte Benutzer. Wenn Sie ein trust-based, offenes, lokales Netzwerk ungeschützt dem in höchstem Grad unsicheren Internet aussetzen, ist das so, als wenn Sie Ihre Haustür in einem unsicheren Vorort offenlassen — für eine Weile mag nichts passieren, aber *eventuell* wird sich jemand die Gelegenheit zu Nutze machen.

2.2.1.1. Broadcast-Netzwerke

Systemadministratoren vernachlässigen oftmals die Bedeutung vernetzter Hardware in ihren Sicherheitssystemen. Einfache Hardware wie z.B. Hubs und Router arbeiten nach dem Broadcast oder ungeschaltetem Prinzip; d.h. wenn ein Knoten Daten über ein Netzwerk überträgt, sendet die Hub oder der Router die Datenpakete solange, bis der Empfängerknoten die Daten empfangen und verarbeitet hat. Diese Methode ist am anfälligsten für *ARP* (Address Resolution Protocol) oder *MAC* (Media Access Control) Spoofing durch außenstehende Angreifer oder unbefugte Benutzer in lokalen Knoten.

2.2.1.2. Zentralisierte Server

Eine weitere Netzwerkfalle ist die Verwendung zentralisierter Rechner. Eine beliebte Maßnahme zur Kostensenkung für Firmen ist es, alle Dienste auf einer einzigen, leistungsstarken Maschine zusammenzuführen. Dies ist bequem, da einfacher zu verwalten und es kostet wesentliche weniger als Multiple-Server-Konfigurationen. Ein zentralisierter Server bildet jedoch auch einen Fehlerpunkt im Netzwerk. Wird der zentrale Server beschädigt, kann dadurch das gesamte Netzwerk nutzlos oder gar zur Angriffsfläche für Datenmanipulation oder Diebstahl werden. In diesen Fällen wird ein zentraler Server zur offenen Tür und erlaubt Zugang zum gesamten Netzwerk.

2.3. Bedrohungen der Serversicherheit

Serversicherheit ist genauso wichtig wie Netzwerksicherheit, da Server meistens einen Großteil der unternehmenskritischen Informationen halten. Wird ein Server beeinträchtigt, kann der Cracker auf den gesamten Inhalt zugreifen und nach Belieben Daten stehlen oder manipulieren. Die folgenden Abschnitte behandeln die wichtigsten Punkte.

2.3.1. Unbenutzte Dienste und offene Ports

Eine Komplettinstallation von Red Hat Enterprise Linux enthält über 1000 Applikationen und Bibliotheken. Die meisten Systemadministratoren wählen jedoch nicht jedes einzelne Paket zur Installation

aus, sondern ziehen es vor, eine Basis-Installation von Paketen inklusive mehrerer Serverapplikationen durchzuführen.

Ein häufig anzutreffendes Verhalten unter Systemadministratoren ist es, das Betriebssystem zu installieren, ohne darauf zu achten, welche Programme eigentlich installiert werden. Dies kann problematisch werden, da eventuell unbenötigte Dienste installiert werden, die mit den Standard-Einstellungen konfiguriert und standardmäßig aktiviert werden. Dies kann dazu führen, dass unerwünschte Dienste wie Telnet, DHCP oder DNS auf einem Server oder einer Workstation laufen, ohne dass der Systemadministrator es merkt, was wiederum zu unerwünschtem Verkehr zum Server oder zur Hintertür für Cracker in das System werden kann. Weitere Informationen zum Schließen von Ports und Deaktivieren unbenutzer Dienste finden Sie unter Kapitel 5.

2.3.2. Dienste ohne Patches

Die meisten Serverapplikationen, die in einer Standard-Installation enthalten sind, sind solide, gründlich getestete Softwareapplikationen. Dadurch, dass diese viele Jahre in Produktionsumgebungen eingesetzt wurden, ist ihr Code ausgereift und viele Fehler sind gefunden und behoben worden.

So etwas wie perfekte Software gibt es jedoch nicht, es ist immer Platz für weitere Verbesserungen. Desweiteren ist neuere Software nicht immer so durchgängig getestet wie man erwarten würde, z.B. dadurch, dass diese erst seit kurzem in der Produktionsumgebung eingesetzt wird oder weil diese noch nicht ganz so beliebt ist wie andere Server-Software.

Entwickler und Systemadministratoren finden häufig ausbeutbare Fehler in Serverapplikationen und veröffentlichen diese Informationen auf Bug-Tracking und sicherheitsbezogenen Webseiten wie die Bugtraq-Mailingliste (http://www.securityfocus.com) oder die Webseite des Computer Emergency Response Team (CERT) (http://www.cert.org). Auch wenn diese Mechanismen eine effektive Methode zur Warnung der Community vor Sicherheitsproblemen darstellt, liegt es letztendlich an den Systemadministratoren, ihre Systeme sofort mit einem Patch zu versehen. Dies ist insbesondere wichtig, da Cracker auch Zugang zu den gleichen Tracking-Dienste haben und diese Informationen ausnutzen, um nicht gepatchte Systeme zu cracken. Eine gute Systemadministration verlangt Wachsamkeit, andauerndes Fehlertracking und vernünftige Systemwartung für eine sichere Rechenumgebung.

Weitere Informationen dazu, wie Sie ein System immer auf den aktuellen Stand bringen können, finden Sie unter Kapitel 3.

2.3.3. Unaufmerksame Administration

Administratoren, die Systeme nicht mit den neuesten Patches versehen, stellen eine der größten Bedrohungen für die Serversicherheit dar. Nach Angaben des *System Administration Network and Security Institute* (*SANS*) ist der Hauptgrund für Computersicherheitsprobleme "untrainierte Mitarbeiter, die mit der Wartung der Sicherheit betraut werden, ohne richtiges Training oder die nötige Zeit, um den Job ordnungsgemäß auszuführen."[1] Dies trifft sowohl auf unerfahrene Administratoren als auch auf vermessene oder unmotivierte Administratoren zu.

Einige Administratoren vergessen ihre Server oder Workstations zu patchen, während andere vergessen, Log-Mitteilungen vom Systemkernel oder Netzwerkverkehr zu beobachten. Ein weiterer häufiger Fehler ist, standardmäßige Standardpasswörter oder Schlüssel für Dienste so zu belassen, wie sie sind. So haben zum Beispiel einige Datenbanken standardmäßige Administrationspasswörter, weil die Datenbankentwickler annehmen, dass der Systemadministrator diese sofort nach der Installation ändert. Vergisst nun ein Systemadministrator, diese Passwörter zu ändern, können sogar unerfahrene Cracker mit einem weitverbreiteten Standard-Passwort auf administrative Privilegien dieser Datenbank zugreifen. Dies sind nur einige Beispiele dafür, wie unaufmerksame Administration zu unsicheren Servern führen kann.

1. Quelle: http://www.sans.org/newlook/resources/errors.html

2.3.4. Von Natur aus unsichere Dienste

Auch das wachsamste Unternehmen kann Opfer von Schwachstellen werden, wenn die gewählten Netzwerkdienste von Natur aus unsicher sind. Es werden zum Beispiel viele Dienste unter der Annahme entwickelt, dass diese über sichere Netzwerke verwendet werden; diese Annahme schlägt jedoch fehl, sobald diese Dienste über das Internet verfügbar gemacht werden — welches in sich unsicher und vertrauensunwürdig ist.

Eine Art von unsicheren Netzwerkdienste ist die, die Benutzernamen und Passwörter für die Authentifizierung benötigt, diese Informationen bei der Übertragung über das Netzwerk jedoch nicht verschlüsselt. Telnet und FTP sind solche Dienste. Paket-Sniffing Software, die den Verkehr zwischen entfernten Benutzern und einem solchen Server überwacht, kann dann einfach die Benutzernamen und Passwörter stehlen.

Die oben genannten Dienste können auch leichter einer im Industriejargon *Man-in-the-Middle* genannten Attacke zum Opfer fallen. Bei dieser Art Angriff leitet ein Cracker den Netzwerkverkehr um, indem er einen gecrackten Name-Server austrickst, auf seinen Rechner zu weisen und nicht auf den eigentlichen Server. Sobald dann jemand eine Remote-Session zu dem Server öffnet, verhält sich der Rechner vom Angreifer als unsichtbare Leitung, und sitzt leise zwischen dem Remote-Service und dem ahnungslosen Benutzer, und sammelt Informationen. Auf diese Weise kann ein Cracker Administrations-Passwörter und Daten sammeln, ohne das der Server oder der Benutzer dies merkt.

Ein weiteres Beispiel für unsichere Dienste sind Netzwerkdateisysteme und Informationssysteme wie zum Beispiel NFS oder NIS, die ausdrücklich für eine Verwendung in LANs entwickelt wurden und dann jedoch für WANs erweitert wurden (für entfernte Benutzer). NFS hat standardmäßig keine Authentifizierungs- oder Sicherheitsmechanismen konfiguriert, um Cracker vom Mounten des NFS-Shares und Zugang zu allem, was darin enthalten ist, abzuhalten. NIS verfügt auch über wichtige Informationen, die jedem Computer im Netzwerk bekannt sein müssen, einschließlich Passwörter und Dateiberechtigungen innerhalb einer Nur-Text ASCII oder DBM (ASCII-abgeleiteten) Datenbank. Ein Cracker, der Zugang zu dieser Datenbank erhält, kann dann auf jeden Benutzeraccount in diesem Netzwerk zugreifen, einschließlich dem des Administrators.

Standardmäßig sind bei Red Hat Enterprise Linux solche Dienste deaktiviert. Da Administratoren häufig jedoch zur Verwendung dieser Dienste gezwungen sind, ist Sorgfalt von oberster Wichtigkeit. Weitere Informationen zum sicheren Einrichten eines Servers finden Sie unter Kapitel 5.

2.4. Bedrohungen der Workstation- und Heim-PC-Sicherheit

Workstations und Heim-PCs sind nicht ganz so anfällig für Attacken wie Netzwerke oder Server, da sie jedoch häufig empfindliche Informationen wie zum Beispiel Kreditkartendaten enthalten, werden sie schnell zum Ziel von Crackern. Workstations können kooptiert werden, ohne das der Benutzer dies merkt, und von Angreifern als "Sklaven"-Maschinen für koordinierte Angriffe verwendet werden. Aus diesem Grund kann die Kenntnis der Schwachstellen einer Workstation Benutzern den Kopfschmerz der Neuinstallation eines Betriebssystems oder das Erholen nach einem Datendiebstahl ersparen.

2.4.1. Ungeeignete Passwörter

Schlechte Passwörter ist einer der leichtesten Methoden für einen Angreifer, Zugang zu einem System zu erhalten. Weitere Informationen zur Vermeidung der Fallen bei der Erstellung von Passwörtern finden Sie unter Abschnitt 4.3.

2.4.2. Anfällige Client-Applikationen

Auch wenn ein Administrator über einen sicheren und gepatchten Server verfügt, heißt dies noch lange nicht, dass Remote-Benutzer sicher sind, wenn sie auf diesen zugreifen. Wenn zum Beispiel der Server Telnet oder FTP-Dienste über ein öffentliches Netzwerk zur Verfügung stellt, kann ein Angreifer die

Nur-Text Benutzernamen und Passwörter abgreifen, wenn diese über das Netzwerk übertragen werden, und dann diese Account-Informationen zum Zugriff auf die Workstation des Remote-Benutzers missbrauchen.

Selbst wenn sichere Protokolle wie z.B. SSH verwendet werden, kann ein Remote-Benutzer anfällig für bestimmte Attacken sein, wenn ihre Client-Applikationen nicht auf dem neuesten Stand sind. So kann zum Beispiel ein v.1 SSH Client anfällig sein für eine X-Forwarding Attacke eines böswilligen SSH-Servers. Sobald dieser mit dem Server verbunden ist, kann der Angreifer leise sämtliche Tastatureingaben und Mausklicks des Benutzers im Netzwerk registrieren. Dieses Problem wurde im v.2 SSH-Protokoll behoben, es liegt jedoch am Benutzer, festzustellen, welche Applikationen solche Anfälligkeiten aufweisen und diese wenn nötig auf den neuesten Stand zu bringen.

Kapitel 4 beschreibt im Detail, welche Schritte Administratoren und Heimanwender einleiten sollten, um die Anfälligkeit von Computer-Workstations einzuschränken.

II. Red Hat Enterprise Linux für Sicherheit konfigurieren

Dieser Abschnitt informiert Administratoren über die richtigen Methoden und Tools, die zur Sicherung von Red Hat Enterprise Linux Workstations, Red Hat Enterprise Linux Servern und Netzwerk-Ressourcen verwendet werden sollten. Weiter beschreibt dieser, wie sichere Verbindungen hergestellt werden, Ports und Services blockiert werden und aktive Filter zur Vorbeugung von Netzwerkeindringungen einzurichten sind.

Inhaltsverzeichnis

3. Sicherheits-Updates 17
4. Workstation-Sicherheit 23
5. Server-Sicherheit 43
6. Virtuelle Private Netzwerke 57
7. Firewalls 67

Kapitel 3.

Sicherheits-Updates

Wenn Sicherheitsrisiken in einer Software entdeckt werden, muss die Software geändert werden, um das mögliche Sicherheitsrisiko auszuschließen. Ist das Paket Teil einer Red Hat Enterprise Linux Distribution, die derzeit unterstützt wird, liegt es im Interesse von Red Hat, Inc., so schnell wie möglich aktualisierte Pakete herauszugeben, die Sicherheitslöcher stopfen. Wird die Mitteilung eines Sicherheitsrisikos von einem Patch begleitet (oder Code, der den Fehler behebt), wird der Patch auf das Red Hat Enterprise Linux Paket angewandt, von unserem Qualitätssicherungsteam getestet und als Errata-Update herausgegeben. Enthält die Ankündigung keinen Patch, arbeitet ein Red Hat Entwickler mit dem Herausgeber des Pakets zusammen, um das Problem zu lösen. Wurde das Problem behoben, wird das Paket getestet und als Errata-Update herausgegeben.

Wenn Sie ein Paket verwenden, für das ein Sicherheits-Errata-Report herausgegeben wurde, wird strengstens empfohlen, dass Sie Ihre Sicherheits-Errata-Pakete sobald wie möglich aktualisieren, um die Zeit, die Ihr System angreifbar ist, zu minimieren..

3.1. Pakete aktualisieren

Wenn Sie Pakete auf Ihrem System aktualisieren, ist es wichtig, das Update von einer vertrauenswürdigen Quelle herunterzuladen. Ein Cracker kann leicht eine Version eines Paketes nachbauen (mit der gleichen Versionsnummer des Pakets, das theoretisch das Problem lösen sollte), mit einem anderen Sicherheitsrisiko im Paket, und dieses im Internet veröffentlichen. Falls dies geschieht, kann durch Sicherheitsmaßnahmen wie das Abgleichen der Pakete gegen die ursprünglichen RPMs dieses Risiko nicht entdeckt werden. Es ist daher wichtig, dass Sie RPMs nur von Quellen wie Red Hat, Inc. herunterladen und die Signatur des Pakets prüfen, um sicherzustellen, dass es wirklich von dieser Quelle entwickelt wurde.

Red Hat bietet zwei Möglichkeiten, um Informationen über Sicherheitsupdates zu erhalten:

1. Gelistet und erhältlich zum Download von Red Hat Network
2. Gelistet und ungelinkt auf der Red Hat Errata-Webseite

Hinweis

Mit der Red Hat Enterprise Linux Produktlinie beginnend, können aktualisierte Pakete nur von Red Hat Network heruntergeladen werden. Obwohl die Red Hat Errata Website aktualisierte Informationen enthält, so enthält diese nicht die eigentlichen Download-Pakete.

3.1.1. Red Hat Network benutzen

Red Hat Network ermöglicht Ihnen, den größten Teil des Update-Prozesses zu automatisieren. Es stellt fest, welche RPM-Pakete für Ihr System benötigt werden, lädt diese von einer sicheren Quelle herunter, prüft die RPM-Signatur, um festzustellen, ob diese nicht unbefugt geändert wurden, und aktualisiert diese. Die Paketinstallation kann sofort erfolgen oder auf einen bestimmten Zeitpunkt verlegt werden.

Red Hat Network benötigt von Ihnen ein *Systemprofil* von jeder Maschine, die aktualisiert werden soll. Dieses Systemprofil enthält Hardware- und Softwareinformationen über das System. Diese Informationen werden vertraulich behandelt und werden an niemanden weitergegeben. Sie werden nur

benötigt, um festzustellen, welche Errata-Updates auf Ihr System angewendet werden können. Ohne diese kann Red Hat Network nicht feststellen, ob Ihr System aktualisiert werden muss. Wenn ein Sicherheits-Errata (oder ein anderes Errata) herausgegeben wird, schickt Red Hat Network Ihnen eine E-Mail mit einer Beschreibung der Errata, sowie eine Liste mit Informationen, welche Teile Ihres Systems betroffen sind. Um das Update anzuwenden, können Sie den **Red Hat Update Agent** verwenden oder ein Update über die Webseite http://rhn.redhat.com planen.

Tipp

Red Hat Enterprise Linux enthält das **Red Hat Network Alert Notification Tool**, ein Symbol im Panel, das sichtlich Hinweise für verfügbare Updates für ein Red Hat Enterprise Linux-System anzeigt. Weitere Informationen über das Applet finden Sie unter folgender URL: http://rhn.redhat.com/help/basic/applet.html

Weitere Informationen zu den Vorteilen des Red Hat Network finden Sie im *Red Hat Network Reference Guide* unter http://www.redhat.com/docs/manuals/RHNetwork/ oder besuchen Sie http://rhn.redhat.com.

Wichtig

Bevor Sie jegliche Sicherheits-Errata installieren, stellen Sie sicher, dass Sie alle Anweisungen im Errata-Report gelesen und diese genau befolgt haben. Allgemeine Anweisungen über das Anwenden von Änderungen durch ein Errata-Update finden Sie unter Abschnitt 3.1.5.

3.1.2. Verwenden der Red Hat Errata-Webseite

Wenn Sicherheits-Errata-Berichte veröffentlicht werden, werden diese auf der Red Hat Errata-Webseite unter http://www.redhat.com/apps/support/errata/ bekanntgegeben. Sie können auf dieser Seite das Produkt und die Version für Ihr System auswählen und dann **Security** oben auf der Seite auswählen, um nur Red Hat Enterprise Linux Sicherheitsinformationen anzuzeigen. Beschreibt die Zusammenfassung in einer dieser Informationen ein Paket, das auf Ihrem System verwendet wird, klicken Sie auf die Zusammenfassung für weitere Details.

Die Detail-Seite beschreibt das Sicherheitsproblem und gibt alle nötigen Anweisungen, die zusätzlich zur Aktualisierung des Pakets befolgt werden müssen, um das Sicherheitsloch zu stopfen.

Um das/die aktualisierte(n) Paket(e) herunterzuladen, klicken Sie auf den Paketnamen und speichern Sie diese(s) auf der Festplatte. Es wird dringend empfohlen, dass Sie ein neues Verzeichnis, wie z.B. `/tmp/updates` erstellen und dort die heruntergeladenen Pakete speichern.

3.1.3. Signierte Pakete verifizieren

Alle Red Hat Enterprise Linux Pakete sind signiert mit dem Red Hat, Inc. *GPG*-Schlüssel. GPG steht für GNU Privacy Guard oder GnuPG, einem freien Softwarepaket, welches dazu dient, die Authentizität von Dateien zu gewährleisten. Zum Beispiel: Ein Private Key (Secret Key) von Red Hat hält das Paket verschlossen, wohingegen der Public Key das Paket verifiziert und freischaltet. Im Falle, dass der Public Key, vertrieben durch Red Hat nicht mit dem Private Key im Laufe der RPM-Verifizierung übereinstimmt, so kann dies bedeuten, dass das Paket in irgendeiner Form geändert worden ist und dies ein Sicherheitsrisiko darstellen könnte.

Die RPM-Utility in Red Hat Enterprise Linux versucht automatisch die GPG Signatur einer RPM vor der Installation zu verifizieren. Wenn der Red Hat GPG-Schlüssel noch nicht installiert worden ist,

dann sollten Sie diesen jetzt von einer sicheren, statischen Quelle wie einer Red Hat Enterprise Linux CD-ROM installieren.

Unter der Annahme, das die CD-ROM in `/mnt/cdrom` gemountet ist, können Sie den folgenden Befehl zum Importieren des Schlüssels in den *Keyring* oder Schlüsselring verwenden (eine Datenbank bestehend aus zuverlässigen Schlüsseln auf dem System).

```
rpm --import /mnt/cdrom/RPM-GPG-KEY
```

Um eine Liste aller installierten Schlüssel für die RPM-Verifikation anzuzeigen, führen Sie folgenden Befehl aus:

```
rpm -qa gpg-pubkey*
```

Für den Red Hat Schlüssel enthält das Output folgendes:

```
gpg-pubkey-db42a60e-37ea5438
```

Um Details über einen bestimmten Schlüssel anzuzeigen, verwenden Sie den Befehl `rpm -qi`, gefolgt vom Output des vorhergehenden Befehls:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

Es ist von größter Wichtigkeit, dass Sie die Signatur der RPM-Dateien verifizieren, bevor Sie diese installieren. Dieser Schritt versichert Ihnen, dass die RPMs der Red Hat, Inc. Version nicht verändert wurden. Um alle heruntergeladenen Pakete gleichzeitig zu prüfen, geben Sie folgenden Befehl ein:

```
rpm -K /tmp/updates/*.rpm
```

Für jedes einzelne Paket erhalten Sie im Falle einer erfolgreichen Verifikation den Output `gpg OK`. Falls dies nicht der Fall ist, so überprüfen Sie, ob Sie den richtigen Red Hat Public Key verwenden und verifizieren Sie die Quelle des Inhalts. Pakete, welche die GPG-Verifizierung nicht bestehen, sollten nicht installiert werden, da die Möglichkeit besteht, dass diese von einem Dritten verändert wurden.

Nachdem der GPG-Schlüssel verifiziert und alle Pakete im Zusammenhang mit dem Errata-Bericht heruntergeladen wurden, können Sie diese als Root angemeldet in einem Shell-Prompt installieren.

3.1.4. Signierte Pakete installieren

Die Installation für die meisten Pakete kann sicher durch den folgenden Befehl erfolgen (Kernel-Pakete ausgenommen):

```
rpm -Uvh /tmp/updates/*.rpm
```

Für Kernel-Pakete sollten Sie den folgenden Befehl verwenden:

```
rpm -ivh /tmp/updates/<kernel-package>
```

Ersetzen Sie *<kernel-package>* im vorhergehenden Beispiel mit dem Namen der Kernel-RPM.

Nachdem die Maschine mithilfe des neuen Kernels sicher neu gestartet ist, kann der alte Kernel mit dem folgenden Befehl entfernt werden:

```
rpm -e <old-kernel-package>
```

Ersetzen Sie *<old-kernel-package>* im vorhergehenden Beispiel mit dem Namen der älteren Kernel-RPM.

Hinweis

Es ist keine Voraussetzung, dass der alte Kernel entfernt wird. Der standardmäßige Boot Loader, GRUB, erlaubt die Installation mehrerer Kernel, welche dann von einem Menü während des Bootvorganges ausgewählt werden können.

Wichtig

Bevor Sie jegliche Sicherheits-Errata installieren, stellen Sie sicher, dass Sie alle Anweisungen im Errata-Report gelesen und diese genau befolgt haben. Allgemeine Anweisungen über das Anwenden von Änderungen durch ein Errata-Update finden Sie unter Abschnitt 3.1.5.

3.1.5. Anwenden der Änderungen

Nachdem Sie die Sicherheitserrata über das Red Hat Network oder die Red Hat Errata-Webseite heruntergeladen und installiert haben, ist es wichtig, die ältere Software zu stoppen und die neue Software zu verwenden. Die Vorgehensweise hängt von der Art der Software ab, die aktualisiert wurde. Die folgende Liste stellt die allgemeinen Kategorien der Software dar und gibt Anweisungen für das Verwenden der aktualisierten Versionen nach einem Paket-Upgrade.

Hinweis

Im allgemeinen ist ein Neustart der beste Weg, sicherzustellen, dass die aktuellste Version eines Softwarepakets verwendet wird. Diese Option ist jedoch nicht immer für den Systemadministrator verfügbar.

Applikaitonen

User-Space Applikationen sind alle Programme, die durch einen Systembenutzer ausgelöst werden. Gewöhnlicherweise werden diese Applikationen nur verwendet, wenn ein Benutzer, ein Skript oder ein automatisierter Task diese startet und nicht lange ausführt.

Wird solch eine Applikation aktualisiert, stoppen Sie alle Instanzen dieser Applikation auf dem System und starten Sie das Programm neu, um die aktualisierte Version zu verwenden.

Kernel

Der Kernel ist die Kern-Softwarekomponente für das Red Hat Enterprise Linux Betriebssystem. Er verwaltet den Zugang zum Speicher, zum Prozessor und zu Peripheriegeräten, sowie plant alle Aufgaben.

Durch dessen zentrale Rolle kann der Kernel nur durch ein Herunterfahren des Computers neu gestartet werden. Daher kann eine aktualisierte Version des Kernels nicht verwendet werden, bis das System neu gestartet wird.

Shared-Bibliotheken

Shared-Bibliotheken sind Einheiten von Code, wie z.B. `glibc`, die von einer Reihe von Applikationen und Softwareprogrammen gemeinsam verwendet werden. Applikationen, die Shared-Bibliotheken verwenden, laden normalerweise den gemeinsamen Code beim Starten der Applikation, so dass alle Applikationen, die die aktualisierte Bibliothek verwenden, neu gestartet werden müssen.

Um festzustellen, welche laufenden Applikationen mit einer bestimmten Bibliothek verknüpft sind, verwenden Sie den Befehl `lsof` wie im folgenden Beispiel:

```
lsof /usr/lib/libwrap.so*
```

Dieser Befehl gibt eine Liste aller laufenden Programme aus, die TCP Wrappers für die Host-Zugangskontrolle verwenden. Alle aufgelisteten Programme müssen angehalten und neu gestartet werden, wenn das `tcp_wrappers`-Paket aktualisiert wird.

SysV Services

SysV Services sind beständige Server-Programme, die während es Bootens gestartet werden. Beispiele für SysV Services sind `sshd`, `vsftpd` und `xinetd`.

Da sich diese Programme normalerweise im Speicher aufhalten, solange die Maschine gebootet wird, muss jeder aktualisierte SysV Service nach dem Upgrade des Pakets angehalten und neu gestartet werden. Dies kann über das **Services Configuration Tool** oder durch das Anmelden an einem Shell-Prompt und Eingeben des Befehls `/sbin/service` wie im folgenden Beispiel:

```
/sbin/service <service-name> restart
```

Ersetzen Sie im vorhergehenden Beispiel *<service-name>* mit dem Namen des Services, wie z.B. `sshd`.

Im Kapitel *Zugangskontrolle für Services* im*Red Hat Enterprise Linux Handbuch zur System-Administration* finden Sie weitere Informationen zum **Services Configuration Tool**.

`xinetd` Services

Services, die vom Super-Service `xinetd` verwaltet werden, werden nur ausgeführt, wenn eine aktive Verbindung vorliegt. Beispiele von Services, die von `xinetd` gesteuert werden, sind Telnet, IMAP und POP3.

Da neue Instanzen dieser Services durch `xinetd` jedesmal gestartet werden, wenn eine neue Anfrage empfangen wird, werden die Verbindungen, die nach einem Upgrade entstehen, durch die aktualisierte Software verwaltet. Bestehen jedoch aktive Verbindungen zur der Zeit, zu der von `xinetd` verwaltete Services aktualisiert werden, werden diese von der älteren Version der Software verwaltet.

Um ältere Instanzen eines bestimmten `xinetd`-Services zu stoppen, aktualisieren Sie das Paket für den Service und stoppen Sie dann alle Prozesse, die zur Zeit laufen. Prüfen Sie zuerst welche Prozesse laufen mit dem Befehl `ps` und geben Sie dann den Befehl `kill` oder `killall` ein, um alle aktuellen Instanzen dieses Service zu stoppen.

Wenn zum Beispiel Sicherheits-Errata `imap`-Pakere herausgegeben werden, aktualisieren Sie die Pakete und geben Sie folgenden Befehl als root ein:

```
ps -aux | grep imap
```

Dieser Befehl gibt alle aktiven IMAP-Sitzungen aus. Individuelle Sitzungen können dann durch den folgenden Befehl beendet werden:

```
kill -9 <PID>
```

Ersetzen Sie im vorhergehenden Beispiel *<PID>* durch die Prozess-Identifikationsnummer (zu finden in der zweiten Spalte des `ps` Befehls) für eine IMAP-Sitzung.

Um alle aktiven IMAP-Sitzungen zu beenden, geben Sie den folgenden Befehl ein:

```
killall imapd
```

Im Kapitel *TCP Wrappers und* `xinetd` im *Red Hat Enterprise Linux Referenzhandbuch* finden Sie weitere Informationen zu `xinetd`.

Kapitel 4.

Workstation-Sicherheit

Die Sicherung einer Linux-Umgebung beginnt mit der Workstation. Egal ob Sie Ihren persönlichen Rechner oder ein Firmensystem sichern, eine vernünftige Sicherheitspolice beginnt mit dem einzelnen Computer. Im Endeffekt ist ein Computernetzwerk nur so sicher wie das schwächste Mitglied.

4.1. Auswertung der Workstation-Sicherheit

Wenn Sie die Sicherheit einer Red Hat Enterprise Linux Workstation auswerten, sollten Sie folgendes untersuchen:

- *BIOS und Bootloader-Sicherheit* — Kann ein unbefugter Benutzer physisch auf den Rechner zugreifen und in den Einzelbenutzer- oder Rettungsmodus booten, ohne dass nach einem Passwort gefragt wird?
- *Passwort-Sicherheit* — Wie sicher sind die Passwörter für die Benutzeraccounts auf dem Computer?
- *Administrative Kontrolle* — Wer hat alles einen Account auf dem System, und wieviel administrative Kontrolle ist ihnen zugewiesen?
- *Verfügbare Netzwerk-Dienste* — Welche Dienste hören das Netzwerk nach Anfragen ab, und sollten diese wirklich alle aktiv sein?
- *Persönliche Firewalls* — Welche Art von Firewall, wenn überhaupt, ist nötig?
- *Kommunikationstools mit erweiterter Sicherheit* — Welche Tools sollten zur Kommunikation zwischen Workstations verwendet werden, und welche sollten vermieden werden?

4.2. BIOS und Bootloader Sicherheit

Passwort-Schutz für das BIOS (oder BIOS-Äquivalent) und den Bootloader kann unbefugte Benutzer, die physikalischen Zugang zu Ihren Systemen haben, davon abhalten, externe Medien zu booten oder sich durch den Einzelbenutzermodus als root anzumelden. Die Sicherheitsmaßnahmen, die man durchführen sollte, um vor solchen Attacken geschützt zu sein, hängt zum einen von den Informationen ab, die auf der Workstation gespeichert sind und zum anderen vom Aufstellungsort des Rechners.

Wenn zum Beispiel ein Computer auf einer Messe verwendet wird und keine empfindlichen Daten enthält, ist es nicht unbedingt kritisch, solche Attacken zu verhindern. Wenn jedoch ein Laptop eines Mitarbeiters mit privaten, nicht-passwortgeschützten SSH-Schlüsseln zum Firmennetzwerk auf der gleichen Messe unbeaufsichtigt gelassen wird, kann dies zu einem bedeutenden Sicherheitsbruch führen, der Auswirkungen auf das gesamte Unternehmen haben kann.

Wenn auf der anderen Seite sich die Workstation an einem Ort befindet, zu dem nur befugte oder vertrauenswürdige Personen Zugang haben, ist das Sichern des BIOS oder des Bootloaders nicht unbedingt von Nöten.

4.2.1. BIOS-Passwörter

Die folgenden sind die zwei Hauptgründe für den Schutz des BIOS eines Computers durch Passwörter [1]:

1. *Änderungen an den BIOS-Einstellungen verhindern* — Hat ein Eindringling Zugang zum BIOS, kann dieser den Bootvorgang von einer Diskette oder einer CD-ROM festlegen. Dies ermöglicht dann in den Rettungsmodus oder Einzelbenutzermodus zu gelangen und von hier aus schädliche Programme in das System zu pflanzen oder empfindliche Daten zu kopieren.
2. *System-Boot verhindern* — Einige BIOS erlauben Ihnen, den Bootvorgang selbst mit einem Passwort zu schützen. Ist dies aktiviert, muss ein Passwort eingegeben werden, bevor das BIOS den Bootloader startet.

Da die Methoden für das Einstellen von BIOS-Passwörtern sich von Computerhersteller zu Computerhersteller unterscheiden, lesen Sie bitte das Handbuch zu Ihrem Computer für weitere Informationen.

Sollten Sie das BIOS-Passwort vergessen, kann es oft entweder mit Brücken im Motherboard oder durch das Entfernen der CMOS-Batterie zurückgesetzt werden. Daher ist es sinnvoll, wenn möglich, das Computergehäuse abzuschließen. Bevor Sie jedoch diesen Vorgang versuchen, sollten Sie das Handbuch zu Ihrem Computer oder Motherboard lesen.

4.2.1.1. Sicherung von nicht-x86-Plattformen

Andere Plattformen verwenden verschiedene Programme zum Ausführen geringfügiger Aufgaben, die mit denen des BIOS auf einem x86-System äquivalent sind. So verwenden zum Beispiel Intel® Itanium™-basierte Computer die *Extensible Firmware Interface* (*EFI*) Shell.

Anweisungen für den Passwortschutz von BIOS-ähnlichen Programmen auf anderen Architekturen finden Sie in den Anweisungen vom Hersteller.

4.2.2. Bootloader-Passwörter

Hier sind die Hauptgründe, einen Linux-Bootloader mit einem Passwort zu schützen:

1. *Zugang zum Einzelbenutzermodus verhindern* — Wenn Eindringlinge in den Einzelbenutzermodus booten können, werden diese automatisch zu root-Benutzern ohne nach dem root-Passwort gefragt zu werden.
2. *Zugang zur GRUB-Konsole verhindern* — Wenn der Computer GRUB als Bootloader verwendet, kann ein Angreifer die GRUB-Editor-Schnittstelle verwenden, um die Konfiguration zu ändern oder Informationen mithilfe des `cat` Befehls zu sammeln.
3. *Zugang zu unsicheren Betriebssystemen verhindern* — Haben Sie ein Dual-Boot-System, kann ein Angreifer während des Bootens ein Betriebssystem wie zum Beispiel DOS auswählen, das Zugangskontrollen und Dateiberechtigungen ignoriert.

Mit Red Hat Enterprise Linux wird der GRUB Bootloader für die x86 Plattform ausgeliefert. Detaillierte Informationen zu GRUB finden Sie unter dem Titel *der GRUB Bootloader* im *Red Hat Enterprise Linux Referenzhandbuch*.

1. Da sich das System-BIOS von Hersteller zu Hersteller unterscheidet, unterstützen u.U. einige den Passwortschutz beider Typen, während andere vielleicht nur einen Typ und nicht den anderen unterstützen.

4.2.2.1. Passwortschutz für GRUB

Sie können GRUB so konfigurieren, dass die ersten beiden, in Abschnitt 4.2.2 angesprochenen, Probleme adressiert werden, indem Sie eine Passwort-Direktive zur Konfigurationsdatei hinzufügen. Hierfür legen Sie erst ein Passwort fest, öffnen dann einen Shell-Prompt, melden sich als root an und geben folgendes ein:

```
/sbin/grub-md5-crypt
```

Wenn Sie aufgefordert werden, geben Sie das GRUB-Passwort ein und drücken dann [Enter]. Es wird dann ein MD5-Hash des Passworts ausgegeben.

Bearbeiten Sie dann die GRUB-Konfigurationsdatei `/boot/grub/grub.conf`. Öffnen Sie die Datei und fügen Sie die nachfolgende Zeile unterhalb der `timeout` Zeile im Hauptabschnitt des Dokumentes ein:

```
password --md5 <password-hash>
```

Ersetzen Sie *<password-hash>* mit dem Wert, der von `/sbin/grub-md5-crypt`[2] ausgegeben wurde.

Wenn Sie das nächste Mal Ihr System booten, müssen Sie, wenn Sie im GRUB-Menü auf den Editor oder die Befehlszeilen-Schnittstelle zugreifen wollen, erst [p] drücken und dann das GRUB-Passwort eingeben.

Diese Lösung hält jedoch Angreifer nicht davon ab, in ein unsicheres Betriebssystem in einer Dual-Boot-Umgebung zu booten. Hierfür müssen Sie einen anderen Teil der Datei `/boot/grub/grub.conf` bearbeiten.

Suchen Sie die Zeile `title` des unsicheren Betriebssystems und fügen Sie direkt darunter eine Zeile mit dem Befehl `lock` ein.

Für ein DOS-System sollte die Zeile ähnlich wie folgt beginnen:

```
title DOS
lock
```

Achtung

Sie müssen die Zeile `password` im Hauptabschnitt der Datei `/boot/grub/grub.conf` haben, damit dies funktioniert. Ansonsten kann ein Angreifer auf den GRUB-Editor zugreifen und die lock-Zeile entfernen.

Wenn Sie ein anderes Passwort für einen bestimmten Kernel oder ein Betriebssystem festlegen möchten, fügen Sie eine `lock` Zeile gefolgt von einer Passwortzeile in den Abschnitt ein.

Jeder Abschnitt, den Sie mit einem einzigartigen Passwort schützen möchten, sollte mit Zeilen ähnlich dem folgenden Beispiel beginnen:

```
title DOS
lock
password --md5 <password-hash>
```

2. GRUB akzeptiert auch Klartext-Passwörter, es wird jedoch empfohlen, dass Sie die md5-Version verwenden, da `/boot/grub/grub.conf` standardmäßig allgemeine Leseberechtigungen besitzt.

4.3. Passwortsicherheit

Passwörter werden von Red Hat Enterprise Linux als Hauptmethode zur Überprüfung der Benutzeridentität eingesetzt. Aus diesem Grund ist die Passwortsicherheit von erheblicher Bedeutung zum Schutz des Benutzers, der Workstation und dem Netzwerk.

Aus Sicherheitsgründen konfiguriert das Installationsprogramm das System so, dass ein *Message-Digest Algorithm* (*MD5*) und Shadow-Passwörter verwendet werden. Es wird dringend geraten, diese Einstellungen nicht zu verändern.

Wenn Sie die MD5-Passwörter während der Installation deaktivieren, wird das ältere *Data Encryption Standard* (*DES*) Format verwendet. Dieses Format beschränkt Passwörter auf 8 alphanumerische Zeichen (Satzzeichen und andere Sonderzeichen sind nicht erlaubt) und bietet bescheidene 56-bit Verschlüsselung.

Wenn Sie Shadow-Passwörter während der Installation deaktivieren, werden alle Passwörter als One-Way-Hash in der allgemein lesbaren Datei `/etc/passwd` hinterlegt, was das System für Cracker-Attacken offline anfällig macht. Erlangt ein Eindringling Zugang zum Computer als normaler Benutzer, kann dieser die Datei `/etc/passwd` auf seinen eigenen Rechner kopieren und eine beliebige Anzahl Passwort-Knack-Programme darüber laufen lassen. Befindet sich ein unsicheres Passwort in der Datei, ist es nur eine Frage der Zeit, bis diese vom Passwort-Cracker gefunden wird.

Shadow-Passwörter machen diese Art von Angriff unmöglich, da die Passwort-Hashes in der Datei `/etc/shadow` gespeichert werden, die nur vom root-Benutzer gelesen werden kann.

Dies zwingt einen möglichen Angreifer, Passwörter von außen über ein Netzwerkdienste auf dem Rechner wie zum Beispiel SSH oder FTP zu knacken. Diese Art Angriff ist wesentlich langsamer und hinterlässt offensichtliche Spuren, da hunderte von gescheiterten Log-In Versuchen in Systemdateien aufgezeichnet werden. Wenn jedoch der Cracker eine Attacke mitten in der Nacht startet und Sie über schwache Passwörter verfügen, hat der Angreifer eventuell Zugang noch vor Morgengrauen.

Ein weiteres Problem über Format und Speicherung hinaus ist Inhalt. Das wichtigste, was ein Benutzer tun kann, um seinen Account gegen eine Passwort-Attacke zu schützen, ist das Erstellen eines sicheren Passwortes.

4.3.1. Erstellen sicherer Passwörter

Beim Erstellen von Passwörtern ist es hilfreich, die folgenden Richtlinien zu befolgen:

Was Sie nicht tun sollten:

- *Verwenden Sie nicht nur Wörter oder Zahlen* — Sie sollten für ein Passwort nicht nur Wörter oder nur Zahlen verwenden.

  Hier einige Beispiele für schlechte Passwörter:

  - 8675309
  - juan
  - hackme

- *Verwenden Sie keine erkennbaren Wörter* — Wörter wie Namen, im Wörterbuch stehende Wörter oder Begriffe aus Fernsehsendungen oder Romanen sollten vermieden werden, auch wenn diese am Ende mit Zahlen versehen werden.

  Hier einige Beispiele für schlechte Passwörter:

  - john1
  - DS-9

- mentat123

- *Verwenden Sie keine Wörter in anderen Sprachen* — Passwort- Knack-Programme prüfen oft gegen Wortlisten, die Wörterbücher in anderen Sprachen umfassen. Das Verlassen auf Fremdsprachen für sichere Passwörter ist häufig wenig hilfreich.

  Hier einige Beispiele für schlechte Passwörter:

  - cheguevara
  - bienvenido1
  - 1dumbKopf

- *Verwenden Sie keine Hacker-Begriffe* — Wenn Sie denken, Sie sind auf der sicheren Seite, indem Sie Hacker-Begriffe — auch l337 (LEET) genannt — für Ihre Passwörter verwenden, sollten Sie sich das nocheinmal überlegen. Viele Wortlisten enthalten LEET-Begriffe.

  Hier einige Beispiele für schlechte Passwörter:

  - H4X0R
  - 1337

- *Verwenden Sie keine persönlichen Informationen* — Halten Sie sich von persönlichen Informationen fern. Wenn der Angreifer Sie kennt, kann dieser Ihr Passwort leichter herausfinden, wenn das Passwort z.B. folgende Informationen enthält:

  Hier einige Beispiele für schlechte Passwörter:

  - Ihren Namen
  - Den Namen von Haustieren
  - Die Namen von Familienmitgliedern
  - Geburtstage
  - Ihre Telefonnummer oder Postleitzahl

- *Drehen Sie keine erkennbaren Wörter um* — Gute Passwortprogramme drehen gemeinsprachliche Wörter um, das Invertieren von schlechten Passwörtern machen diese also nicht sicherer.

  Hier einige Beispiele für schlechte Passwörter:

  - R0X4H
  - nauj
  - 9-DS

- *Schreiben Sie sich Ihr Passwort nicht auf* — Bewahren Sie Ihr Passwort niemals auf Papier auf. Es ist wesentlich sicherer, sich das Passwort zu merken.
- *Verwenden Sie nie das gleiche Passwort für alle Ihre Rechner* — Es ist wichtig, dass Sie separate Passwörter für jede Maschine erstellen. So sind nicht alle Maschinen auf einen Schlag betroffen, falls ein System einer Attacke zum Opfer fällt.

Was Sie tun sollten:

- *Das Passwort sollte mindestens 8 Zeichen enthalten* — Je länger das Passwort, desto besser. Wenn Sie MD5-Passwörter verwenden, sollten diese 15 Zeichen oder mehr enthalten. DES-Passwörter sollten die maximale Länge haben (acht Zeichen).
- *Mischen Sie Groß- und Kleinbuchstaben* — In Red Hat Enterprise Linuxwerden Groß- und Kleinbuchstaben beachtet, mischen Sie daher Groß- und Kleinschreibung, um die Sicherheit des Passwortes zu erhöhen.
- *Mischen Sie Buchstaben und Zahlen* — Das Hinzufügen von Zahlen, insbesondere in der Mitte des Passwortes (nicht nur am Anfang oder Ende), verstärkt die Sicherheit des Passwortes.
- *Verwenden Sie Sonderzeichen* — Nicht-alphanumerische Zeichen wie z.B. &, $ und > können die Sicherheit des Passwortes erhöhen (dies gilt nicht, wenn Sie DES-Passwörter verwenden).
- *Wählen Sie ein Passwort, das Sie sich leicht merken können* — selbst das beste Passwort hilft Ihnen nicht weiter, wenn Sie sich nicht daran erinnern können. Verwenden Sie daher Akronyme oder andere mnemonische Techniken, um sich das Passwort zu merken.

Durch all diese Regeln erscheint es schwierig, ein Passwort, das all die Kriterien für sichere Passwörter erfüllt, festzulegen. Glücklicherweise gibt es einige einfache Schritte, mit deren Hilfe Sie ein leicht merkbares, sicheres Passwort generieren können.

4.3.1.1. Methodologie zur Erstellung sicherer Passwörter

Es gibt viele verschiedene Methoden, sichere Passwörter zu erstellen. Eine der beliebtesten ist Akronyme. Zum Beispiel:

- Überlegen Sie sich einen einprägsamen Satz, wie zum Beispiel:

  "over the hills and far away, to grandmother's house we go."
- Verwandeln Sie dies als nächstes in ein Akronym (einschließlich der Satzzeichen).

  `othafa,tghwg.`
- Machen Sie das Passwort komplexer, indem Sie Buchstaben durch Zahlen und Sonderzeichen austauschen. Ersetzen Sie zum Beispiel **`t`** durch **`7`** und **`a`** durch **`@`**:

  `o7r@77w,7ghwg.`
- Machen Sie es noch komplexer, indem Sie mindestens einen Buchstaben groß schreiben, zum Beispiel **`H`**.

  `o7r@77w,7gHwg.`
- *Und bitte verwenden Sie nicht unser Beispielpasswort für Ihre Systeme.*

Das Erstellen sicherer Passwörter ist von oberster Wichtigkeit, jedoch genauso wichtig ist das richtige Verwalten der Passwörter, insbesondere für Systemadministratoren in größeren Unternehmen. Im nächsten Abschnitt werden Verfahren für das Erstellen und Verwalten von Benutzerpasswörtern innerhalb eines Unternehmens beschrieben.

4.3.2. Erstellen von Benutzerpasswörtern innerhalb eines Unternehmens

Wenn es eine große Anzahl von Benutzern in einem Unternehmen gibt, haben Systemadministratoren zwei grundlegende Optionen die Verwendung sicherer Passwörter zu forcieren. Sie können entweder

Passwörter für die Benutzer selbst erstellen, oder Benutzer ihre eigenen Passwörter erstellen lassen, und diese dann auf Akzeptanz prüfen.

Das Erstellen von Passwörtern für den Benutzer stellt sicher, dass die Passwörter sicher sind, kann aber schnell zu einer ausufernden Arbeit werden, wenn das Unternehmen wächst. Außerdem erhöht dies das Risiko, dass die Benutzer ihre Passwörter aufschreiben.

Aus diesen Gründen ziehen es Systemadministratoren vor, das die Benutzer ihre eigenen Passwörter erstellen, diese jedoch auf Sicherheit prüfen und in einigen Fällen Benutzer durch Passwort-Aging dazu zu zwingen, ihre Passwörter in periodischen Abständen zu ändern.

4.3.2.1. Forcieren sicherer Passwörter

Um das Netzwerk vor Eindringlingen zu schützen, ist es sinnvoll für Systemadministratoren, sicherzustellen, dass die in einem Unternehmen verwendeten Passwörter sicher sind. Wenn Benutzer aufgefordert werden, ihre eigenen Passwörter zu erstellen oder zu ändern, können sie dies über die Befehlszeilenapplikation `passwd` tun, da dies Kenntnis über den *Pluggable Authentication Manager* (*PAM*) hat, und Sie daher über das PAM-Modul `pam_cracklib.so` prüfen können, ob ein Passwort leicht zu knacken oder zu kurz ist. Da PAM anpassbar ist, ist es möglich, weitere Passwort-Integritätsprüfer wie z.B. `pam_passwdqc` (erhältlich über http://www.openwall.com/passwdqc/) oder Ihr selbstgeschriebenes Modul zu integrieren. Eine Liste erhältlicher PAM-Module finden Sie unter http://www.kernel.org/pub/linux/libs/pam/modules.html. Weitere Informationen zu PAM finden Sie im Kapitel *Pluggable Authentication Modules (PAM)* im *Red Hat Enterprise Linux Referenzhandbuch*.

Es sollte jedoch beachtet werden, dass das Prüfen von Passwörtern zum Erstellungszeitpunkt nicht die effektivste Methode zum Herausfinden unsicherer Passwörter ist. Die Ausführung von Passwort-Cracking-Programmen über alle Passwörter innerhalb der Organisation ist wesentlich effektiver.

Es gibt eine Vielzahl an Passwort-Knack-Programmen, die unter Red Hat Enterprise Linux laufen, jedoch nicht mit dem Betriebssystem ausgeliefert werden. Nachfolgend finden Sie eine kurze Liste der beliebtesten Passwort-Knack-Programme:

Hinweis

Keines dieser Tools wird mit Red Hat Enterprise Linux ausgeliefert, und auch in keiner Weise von Red Hat, Inc. unterstützt.

- ***John The Ripper*** — Ein schnelles und flexibles Passwort-Cracking-Programm. Es ermöglicht die Verwendung mehrerer Wortlisten und Brute-Force Passwort-Cracking. Es ist unter http://www.openwall.com/john/ erhältlich.
- ***Crack*** — die vielleicht bekannteste Passwort-Knack-Software. **Crack** ist auch sehr schnell, jedoch nicht so einfach zu verwenden wie **John The Ripper**. Es ist unter http://www.crypticide.org/users/alecm/ erhältlich.
- ***Slurpie*** — **Slurpie** funktioniert ähnlich wie **John The Ripper** und **Crack**, ist jedoch zum gleichzeitigen Laufen auf mehreren Computern entwickelt und erstellt so eine Distributed Passwort-Cracking Attacke. Es ist erhältlich unter http://www.ussrback.com/distributed.htm.

Achtung

Bitte holen Sie sich stets eine schriftliche Genehmigung ein, bevor Sie Passwörter innerhalb eines Unternehmens zu knacken versuchen.

4.3.2.2. Password Aging

Password Aging ist eine weitere Methode, die von Systemadministratoren verwendet wird, um unsichere Passwörter in einem Unternehmen zu verhindern. Password Aging bedeutet, dass Benutzer nach einer bestimmten Zeit (gewöhnlich 90 Tage) aufgefordert wird, ein neues Passwort festzulegen. Die Theorie dahinter ist, dass wenn ein Benutzer in periodischen Abständen dazu aufgefordert wird, sein Passwort zu ändern, ein geknacktes Passwort einem Cracker nur für eine gewisse Zeit nützlich ist. Der Nachteil von Password Aging ist jedoch, dass Benutzer eher dazu neigen, sich die Passwörter aufzuschreiben.

Es gibt zwei Programme für das Festlegen von Password Aging unter Red Hat Enterprise Linux: den Befehl `chage` oder die grafische Applikation **User Manager** (`system-config-users`).

Die Option `-M` des Befehls `chage` legt die maximale Anzahl von Tagen fest, für die das Passwort gültig ist. Wenn Sie zum Beispiel festlegen wollen, dass ein Benutzer-Passwort nach 90 Tagen ungültig wird, geben Sie den folgenden Befehl ein:

```
chage -M 90 <username>
```

Ersetzen Sie im oben genannten Befehl *<username>* mit dem Namen des Benutzers. Wenn Sie nicht möchten, dass das Passwort ungültig wird, verwenden Sie den Wert `99999` nach der Option `-M` (dies ist etwas mehr als 273 Jahre).

Wenn Sie die grafische Applikation **User Manager** für Password-Aging-Policies verwenden möchten, klicken Sie auf **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Benutzer und Gruppen** oder geben Sie den Befehl `system-config-users` an einem Shell-Prompt ein (z.B. in einem XTerm- oder GNOME-Terminal). Klicken Sie auf den Tab **Benutzer**, wählen Sie den Benutzer aus der Liste aus und klicken Sie auf **Eigenschaften** im Menü (oder wählen Sie **Datei** => **Eigenschaften** aus dem Pull-Down Menü).

Klicken Sie dann auf **Passwort-Info** und geben Sie hier die Anzahl der Tage ein, bevor das Passwort ablaufen soll, wie in Abbildung 4-1 gezeigt.

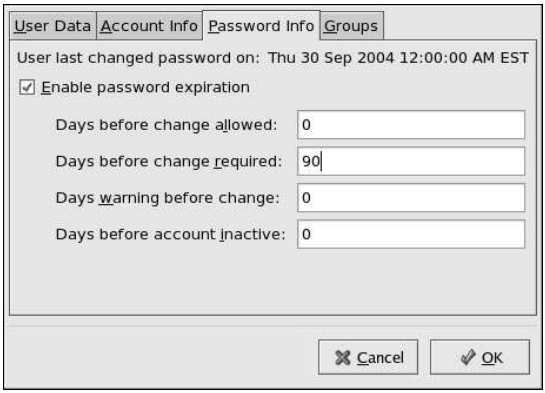

Abbildung 4-1. Passwort-Info Panel

Weitere Informationen zu Benutzern und Gruppen (inklusive Anweisungen für das Erzwingen erstmaliger Passwörter) finden Sie im Kapitel *Benutzer- und Gruppekonfiguration* im *Red Hat Enterprise*

Linux Handbuch zur System-Administration. Einen Überblick über Benutzer- und Ressourcenverwaltung finden Sie im Kapitel *Verwalten von Benutzeraccounts und Zugang zu Ressourcen* im *Red Hat Enterprise Linux Einführung in die System-Administration*.

4.4. Administrative Kontrollen

Für die Verwaltung eines Heim-PCs muss der Benutzer einige Aufgaben als root-Benutzer oder durch effektive root-Berechtigungen durch ein *setuid* Programm wie `sudo` oder `su` ausführen. Ein setuid-Programm arbeitet mit der Benutzer-ID (*UID*) des Besitzers des Programms, und nicht mit der des Benutzers des Programms. Solche Programme werden durch ein kleines `s` im Abschnitt Besitzer einer detaillierten Auflistung wie im folgenden Beispiel markiert:

```
-rwsr-xr-x    1 root     root        47324 May  1 08:09 /bin/su
```

Für Systemadministratoren eines Unternehmens muss festgelegt werden, wieviel administrativen Zugang Benutzer innerhalb des Unternehmens zu ihren Computern haben dürfen. Durch ein PAM-Modul mit dem Namen `pam_console.so` können einige Vorgänge, die normalerweise nur dem root-Benutzer erlaubt sind, wie z.B. das Rebooten und Mounten externer Medien, dem ersten Benutzer, der sich an der physischen Konsole anmeldet, ermöglicht werden (siehe auch das Kapitel *Pluggable Authentication Modules (PAM)* im *Red Hat Enterprise Linux Referenzhandbuch* für weitere Informationen über das `pam_console.so`-Modul). Andere wichtige Systemadministrations-Aufgaben wie das Ändern von Netzwerkeinstellungen, Konfigurieren einer neuen Maus oder das Mounten von Netzwerkgeräten sind jedoch ohne administrativen Zugang nicht möglich, weswegen Systemadministratoren entscheiden müssen, wieviel administrativen Zugang die Benutzer auf ihrem Netzwerk erhalten sollen.

4.4.1. Root-Zugang erlauben

Sind die Benutzer innerhalb eines Unternehmens vertrauenswürdig und kennen sich mit Computern aus, ist das Vergeben von root-Berechtigungen unter Umständen sinnvoll. root-Zugang zu erlauben bedeutet, dass kleinere Probleme wie das Hinzufügen von Geräten oder das Konfigurieren von Netzwerkschnittstellen von den einzelnen Benutzern durchgeführt werden kann und somit Systemadministratoren mehr Zeit für Netzwerksicherheit und andere, wichtige Aufgaben haben.

Auf der anderen Seite kann das Vergeben von root-Rechten zu Einzelbenutzern zu folgenden Problemen führen:

- *Fehlkonfigurationen* — Benutzer mit root-Rechten, können ihre Computer falsch konfigurieren und benötigen dann Hilfe, oder schlimmer noch, können Sicherheitslöcher öffnen, ohne dies zu merken.
- *Unsichere Dienste* — Benutzer mit root-Berechtigungen können unsichere Dienste, wie zum Beispiel FTP oder Telnet auf ihrem Computer laufen lassen, und somit Benutzernamen und Passwörter einem Risiko aussetzen, da diese im Klartext über das Netzwerk verschickt werden.
- *E-Mail-Anhänge als root ansehen* — Wenn auch selten, gibt es doch E-Mail-Viren, die Linux betreffen. Dies wird jedoch nur zum Problem, wenn sie als root ausgeführt werden.

4.4.2. Root-Zugang sperren

Wenn ein Administrator Benutzern keine root-Berechtigungen aus diesen oder anderen Gründen zuweisen möchte, sollte das root-Passwort geheim gehalten und Zugang zu Runlevel 1 oder Einzelbenutzermodus durch Passwortschutz für den Bootloader verhindert werden (weitere Informationen zu diesem Thema finden Sie unter Abschnitt 4.2.2).

Tabelle 4-1 zeigt Methoden, mit denen ein Administrator Anmeldungen als root verhindern kann:

Methode	Beschreibung	Betrifft	Betrifft nicht
Ändern der root-Shell	Bearbeiten Sie die Datei `/etc/passwd` und ändern Sie die Shell von `/bin/bash` zu `/sbin/nologin`.	Verhindert Zugang zur root-Shell und zeichnet den Versuch auf. Die folgenden Programme können nicht mehr auf den root-Account zugreifen: · `login` · `gdm` · `kdm` · `xdm` · `su` · `ssh` · `scp` · `sftp`	Programme, die keine Shell benötigen, wie z.B. FTP-ClientsMail Clients und viele setuid-Programme. Für die folgenden Programme wird der root-Account *nicht* gesperrt: · `sudo` · FTP-Clients · E-Mail Clients
Sperren des root-Zugangs über ein Konsolengerät (tty).	Eine leere `/etc/securetty` Datei verhindert die Anmeldung als root für jegliche Geräte, die am Computer angeschlossen sind.	Verhindert den Zugang zum root-Account über die Konsole oder das Netzwerk. Die folgenden Programme sind für den Zugang zum root-Account gesperrt: · `login` · `gdm` · `kdm` · `xdm` · Andere Netzwerkdienste, die eine tty öffnen	Programme, die sich nicht als root anmelden, aber administrative Aufgaben durch setuid oder andere Mechanismen ausführen. Die folgenden Programme werden *nicht* für den Zugang zum root-Account gesperrt: · `su` · `sudo` · `ssh` · `scp` · `sftp`
Deaktivieren von SSH-Logins als root	Bearbeiten Sie die Datei `/etc/ssh/sshd_config` und setzen Sie den `PermitRootLogin` Parameter auf `no`.	Verhindert root-Zugang über die OpenSSH-Toolsuite. Die folgenden Programme sind für den Zugang zum root-Account gesperrt: · `ssh` · `scp` · `sftp`	Das dies nur die OpenSSH-Toolsuite betrifft, sind keine anderen Programme von dieser Einstellung betroffen.

Methode	Beschreibung	Betrifft	Betrifft nicht
Mit PAM den root - Zugang zu Diensten ein-schränken	Bearbeiten Sie die Datei für den Zieldienst im Verzeichnis `/etc/pam.d/`. Stellen Sie sicher, dass `pam_listfile.so` für die Authentifizierung erforderlich ist. [a]	Verhindert root-Zugang zu Netzwerkdienste, die PAM berücksichtigen. Die folgenden Programme sind für den Zugang zum Rot-Account gesperrt: · FTP-Clients · E-Mail-Clients · `login` · `gdm` · `kdm` · `xdm` · `ssh` · `scp` · `sftp` · Alle anderen Dienste, die PAM berücksichtigen	Programme und Dienste, die PAM nicht berücksichtigen.
Bemerkungen: a. Weitere Informationen finden Sie unter Abschnitt 4.4.2.4.			

Tabelle 4-1. Methoden zum Deaktivieren des root-Accounts

4.4.2.1. Die Root-Shell deaktivieren

Um zu verhindern, dass sich Benutzer direkt als root anmelden, kann der Systemadministrator die Shell des root-Accounts auf `/sbin/nologin` in der Datei `/etc/passwd` setzen. Dies verhindert Zugang zum root-Account über Befehle, die eine Shell benötigen, wie zum Beispiel `su` oder `ssh`.

Wichtig

Programme, die keinen Zugang zur Shell benötigen, wie z.B. E-Mail-Clients oder der Befehl `sudo`, können weiterhin auf den root-Account zugreifen.

4.4.2.2. Root-Anmeldungen deaktivieren

Um den Zugang zum root-Account noch weiter einzuschränken, können Administratoren root-Anmeldungen an der Konsole verhindern, in dem sie die Datei `/etc/securetty` bearbeiten. In dieser Datei werden alle Geräte aufgelistet, auf die der root-Benutzer zugreifen kann. Existiert die Datei nicht, kann sich der root-Benutzer durch ein beliebiges Kommunikationsmedium auf dem System anmelden, sei es über eine Konsole oder eine Raw-Netzwerkschnittstelle. Dies stellt ein Risiko dar, da ein Benutzer sich über Telnet am Computer als root anmelden kann und die Passwörter im Klartext übers Netzwerk versendet. Standardmäßig erlaubt die Red Hat Enterprise Linux-Datei `/etc/securetty` dem root-Benutzer nur, sich an der mit dem Computer direkt verbundenen Konsole anzumelden. Um das Anmelden von root zu verhindern, löschen Sie den Inhalt dieser Datei, indem Sie folgenden Befehl eingeben:

```
echo > /etc/securetty
```

Achtung

Eine leere `/etc/securetty` Datei verhindert *nicht*, dass der root-Benutzer sich von außen über die OpenSSH Toolsuite anmeldet, da die Konsole erst nach der Authentifizierung geöffnet wird.

4.4.2.3. Root SSH-Anmeldungen deaktivieren

Um root-Anmeldungen über das SSH-Protokoll zu verhindern, bearbeiten Sie die Konfigurationsdatei des SSH-Daemons (`/etc/ssh/sshd_config`). Ändern Sie folgende Zeile:

```
# PermitRootLogin yes
```

zu:

```
PermitRootLogin no
```

4.4.2.4. PAM für root deaktivieren

PAM ermöglicht durch das `/lib/security/pam_listfile.so`-Modul eine größere Flexibilität in der Ablehnung bestimmter Accounts. Dies ermöglicht dem Administrator, das Modul an eine Liste von Benutzern zu verweisen, denen die Anmeldung nicht gestattet ist. Unten finden Sie ein Beispiel, wie das Modul für den `vsftpd` FTP-Server in der `/etc/pam.d/vsftpd` PAM-Konfigurationsdatei verwendet werden kann (das \ Zeichen am Ende der ersten Zeile im folgenden Beispiel ist *nicht* nötig, wenn die Direktive auf einer Zeile steht):

```
auth    required    /lib/security/pam_listfile.so    item=user \
sense=deny file=/etc/vsftpd.ftpusers onerr=succeed
```

Dies weist PAM an, die Datei `/etc/vsftpd.ftpusers` zu konsultieren und allen hier aufgeführten Benutzern Zugang zum Dienst zu verbieten. Der Administrator kann den Namen dieser Datei ändern und separate Listen für jeden Dienst oder eine einzige zentrale Liste für die Zugriffsverweigerung für mehrere Dienste führen.

Wenn der Administrator den Zugang zu mehreren Diensten verbieten will, kann eine ähnliche Zeile zum PAM-Konfigurationsdienste wie z.B. `/etc/pam.d/pop` und `/etc/pam.d/imap` für Mail Clients oder `/etc/pam.d/ssh` für SSH-Clients hinzugefügt werden.

Weitere Informationen zu PAM finden Sie im Kapitel *Pluggable Authentication Modules (PAM)* im *Red Hat Enterprise Linux Referenzhandbuch*.

4.4.3. Root-Zugang beschränken

Anstelle dass der Zugang zum root-Benutzer vollständig verweigert wird, kann der Administrator Zugang nur über setuid-Programme wie z.B. `su` oder `sudo` gewähren.

4.4.3.1. Der Befehl `su`

Wenn Sie den Befehl `su` eingeben, wird der Benutzer nach dem root-Passwort gefragt und erhält nach der Authentifizierung ein root-Shell-Prompt.

Wenn über den Befehl `su` angemeldet, *ist* der Benutzer der root-Benutzer und hat absoluten administrativen Zugang zum System. Zusätzlich dazu ist es dem Benutzer mit root-Berechtigungen möglich,

in einigen Fällen den Befehl `su` zu verwenden, um sich als ein anderer Benutzer im System anzumelden, ohne nach einem Passwort gefragt zu werden.

Da dieses Programm sehr mächtig ist, sollten Administratoren innerhalb eines Unternehmens den Zugang zu diesem Befehl beschränken.

Einer der einfachsten Wege ist es, Benutzer zur administrativen Gruppe mit dem Namen *wheel* hinzuzufügen. Hierzu geben Sie den folgenden Befehl als root ein:

```
usermod -G wheel <username>
```

Ersetzen Sie in diesem Befehl `<username>` mit dem Benutzernamen, der zur `wheel`-Gruppe hinzugefügt werden soll.

Um für diesen Zweck das **User Manager** zu verwenden, klicken Sie auf die Schaltfläche **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Benutzer und Gruppen** oder geben Sie den Befehl `system-config-users` an einem Shell-Prompt ein. Wählen Sie den Tab **Benutzer**, wählen Sie den Benutzer aus der Benutzerliste aus und klicken Sie auf **Eigenschaften** aus dem Menü (oder wählen Sie **Datei** => **Eigenschaften** aus dem Pull-Down-Menü).

Wählen Sie dann den Tab **Gruppen** und klicken Sie auf die wheel-Gruppe, wie in Abbildung 4-2 abgebildet.

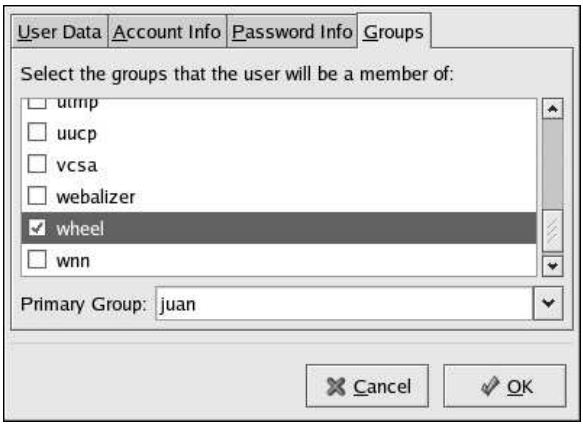

Abbildung 4-2. Das Gruppen-Panel

Öffnen Sie als nächstes die PAM-Konfigurationsdatei für `su` (`/etc/pam.d/su`) in einem Texteditor und entfernen Sie den Kommentar [#] aus der folgenden Zeile:

```
auth  required /lib/security/$ISA/pam_wheel.so use_uid
```

Hierdurch können nur Mitglieder der administrativen Gruppe `wheel` das Programm verwenden.

Hinweis

Der root-Benutzer ist standardmäßig Teil der `wheel`-Gruppe.

4.4.3.2. Der Befehl`sudo`

Der Befehl `sudo` bietet eine weitere Methode, Benutzern administrativen Zugang zu geben. Wenn ein vertrauenswürdiger Benutzer einem administrativen Befehl den Befehl `sudo` voranstellt, wird dieser nach *seinem* Passwort gefragt. Nach der Authentifizierung und vorausgesetzt, dass der Befehl erlaubt ist, wird der administrative Befehl wie von einem root-Benutzer ausgeführt.

Das Format des `sudo`-Befehls ist wie folgt:

```
sudo <command>
```

Im obigen Beispiel würde <*command*> durch einen Befehl, der normalerweise für den root-Benutzer reserviert ist, wie z.B. `mount`, ersetzt.

Wichtig

Alle, die den Befehl `sudo` ausführen, sollten sicherstellen, dass sie abgemeldet sind, bevor sie sich vom Computer entfernen, da der Befehl innerhalb von 5 Minuten nochmal ausgeführt werden kann, ohne dass Sudoers nach einem Passwort gefragt werden. Diese Einstellung kann in der Konfigurationsdatei `/etc/sudoers` geändert werden.

Der `sudo`-Befehl ermöglicht einen höheren Grad an Flexibilität. So können z.B. nur Benutzer, die in der Konfigurationsdatei `/etc/sudoers` aufgeführt sind, den Befehl `sudo` ausführen; dieser Befehl wird dann in der Shell *des Benutzers* ausgeführt, und nicht in der root-Shell. Dies bedeutet, das die root-Shell vollständig deaktiviert werden kann, wie in Abschnitt 4.4.2.1 gezeigt.

Der `sudo`-Befehl liefert auch einen umfangreichen Audit-Trail. Jede erfolgreiche Authentifizierung wird in die Datei `/var/log/messages` und der ausgeführte Befehl, sowie der Benutzername in die Datei `/var/log/secure` geschrieben.

Ein weiterer Vorteil des `sudo`-Befehls ist, dass ein Administrator verschiedenen Benutzern Zugang zu bestimmten Befehlen basierend auf deren Bedürfnissen geben kann.

Administratoren, die die `sudo`-Konfigurationsdatei `/etc/sudoers` bearbeiten wollen, sollten den Befehl `visudo` verwenden.

Um jemandem volle administrative Rechte zu geben, geben Sie `visudo` ein und fügen Sie eine Zeile ähnlich der folgenden in den Abschnitt für die Benutzerrechte ein:

```
juan ALL=(ALL) ALL
```

In diesem Beispiel kann dann der Benutzer `juan` den Befehl `sudo` von jedem Host aus verwenden und jeden Befehl ausführen.

Das untenstehende Beispiel zeigt die mögliche Granularität bei der Konfiguration von `sudo`:

```
%users  localhost=/sbin/shutdown -h now
```

In diesem Beispiel kann jeder Benutzer den Befehl `/sbin/shutdown -h now` ausführen, solange dieser von der Konsole aus eingegeben wird.

Die man-Seite zu `sudoers` enthält eine detaillierte Liste aller Optionen für diese Datei.

4.5. Verfügbare Netzwerkdienste

Während Benutzerzugriff zu administrativen Kontrollen ein wichtiges Thema für Systemadministratoren innerhalb eines Unternehmens ist, ist die Kontrolle der Netzwerkdienste von oberster Wichtigkeit für jeden, der ein Linux-System installiert und anwendet.

Viele Dienste unter Red Hat Enterprise Linux verhalten sich als Netzwerkserver. Wenn ein Netzwerkdienst auf einem Computer ausgeführt wird, hört eine Server-Applikation, auch *Daemon* genannt, auf einem oder mehreren Ports die Verbindungen ab. Jeder dieser Server sollte als potentielle Angriffsstelle betrachtet werden.

4.5.1. Risiken für Dienste

Netzwerkdienste können viele Risiken für Linux-Systeme bedeuten. Untenstehend finden Sie eine Liste der Hauptprobleme:

- *Denial of Service Attacken (DoS)* — In dem ein System mit Anfragen überflutet wird, kann eine Denial of Service Attacke ein System zum völligen Stillstand bringen, da das System versucht, jede Anfrage aufzuzeichnen und zu beantworten.
- *Skript-Anfälligkeits-Attacken* — Wenn ein Server Skripte zum Ausführen von serverseitigen Aufgaben verwendet, kann ein Cracker durch nicht-sachgemäß erstellte Skripte eine Attacke initiieren. Diese Skript-Anfälligkeits-Attacken können zu einem Buffer-Overflow führen oder es dem Angreifer ermöglichen, Dateien auf dem Server zu ändern.
- *Buffer Overflow Attacken* — Dienste, die sich über Ports 0 bis 1023 einwählen, müssen als administrativer Benutzer ausgeführt werden. Hat die Applikation einen ausbeutbaren Buffer Overflow, kann ein Angreifer Zugang zum System erlangen, indem er als Benutzer diesen Daemon ausführt. Da ausbeutbare Buffer-Overflows existieren, können Cracker mit automatisierten Tools das System auf Anfälligkeiten prüfen. Sobald diese dann Zugang zum System haben, können sie mithilfe automatisierter root-Kits den Zugang zum System aufrecht erhalten.

Hinweis

Die Bedrohung durch Schwachstellen, welche durch Puffer-Overflow entstehen, ist in Red Hat Enterprise Linux durch *ExecShield* entschärft, einer ausführbaren Speicher-Segmentation und Schutztechnologie, unterstützt durch x86-kompatible Einzelprozessor- und Multiprozessor-Kernels. ExecShield reduziert das Risiko eines Puffer-Overflow indem virtueller Speicher in ausführbare und nicht-ausführbare Segmente unterteilt wird. Jeglicher Progammcode, welcher versucht ausserhalb des ausführbaren Segments auszuführen (vorsätzlich und böswillig unter Ausnutzung eines Sicherheitsloches in Zusammenhang mit Puffer-Overflow implementierter Code) löst einen Segmentierungsfehler aus und wird abgebrochen.

Execshield beinhaltet auch Unterstützung für *No eXecute* (NX) Technology auf AMD64 Plattformen und *eXecute Disable* (XD) Technologie auf Itanium und Intel® EM64T Systemen. Diese Technologien arbeiten in Zusammenhang mit ExecShield, um böswilligen Code davon abzuhalten, im ausführbaren Bereich des virtuellen Speichers mit einer Granularität von 4 KB ausführbaren Codes abzulaufen, wobei das Risiko eines heimlichen Eindringens in das System unter Ausnuztung eines Puffer-Overflows verringert wird.

Für weitere Informationen über ExecShield und NX oder XD Technologien siehe das Whitepaper mit dem Titel *New Security Enhancements in Red Hat Enterprise Linux v.3, Update 3*, welches unter folgender URL erhältlich ist:

http://www.redhat.com/solutions/info/whitepapers/

Um die Angriffsfläche des Netzwerks zu verringern, sollten alle nicht-genutzten Dienste ausgeschaltet werden.

4.5.2. Identifizieren und Konfigurieren von Diensten

Zur Erhöhung der Sicherheit sind die meisten, mit Red Hat Enterprise Linux installierten Netzwerkdienste standardmäßig deaktiviert, Es gibt jedoch einige nennenswerte Ausnahmen:

- `cupsd` — Der standardmäßige Druck-Server für Red Hat Enterprise Linux.
- `lpd` — Ein alternativer Druck-Server.
- `xinetd` — Ein Super-Server, der die Verbindungen zu einem Host von untergeordneten Servern, wie zum Beispiel `vsftpd` und `telnet` regelt.
- `sendmail` — Der Sendmail Mail Transport Agent ist standardmäßig aktiviert, hört jedoch nur Verbindungen vom localhost ab.
- `sshd` — Der OpenSSH Server, ein sicherer Ersatz für Telnet.

Bei der Entscheidung, ob diese Dienste aktiviert bleiben sollen, sollten Sie mit gesundem Menschenverstand handeln und Vorsicht walten lassen. Wenn Sie zum Beispiel keinen Drucker besitzen, sollten Sie `cupsd` nicht laufen lassen, nur weil Sie eines Tages eventuell einen Drucker kaufen werden. Das gleiche gilt für `portmap`. Wenn Sie keine NFSv3-Volumen mounten oder NIS (den`ypbind` Dienst) nicht verwenden, sollte portmap deaktiviert werden.

Red Hat Enterprise Linux wird mit drei Programmen geliefert, die für das Aktivieren und Deaktivieren von Diensten entwickelt wurden. Aus diesen besteht das **Services Configuration Tool** (`system-config-services`), **ntsysv** und`chkconfig`. Informationen zu diesen Tools finden Sie im Kapitel *Zugangskontrolle zu Diensten* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

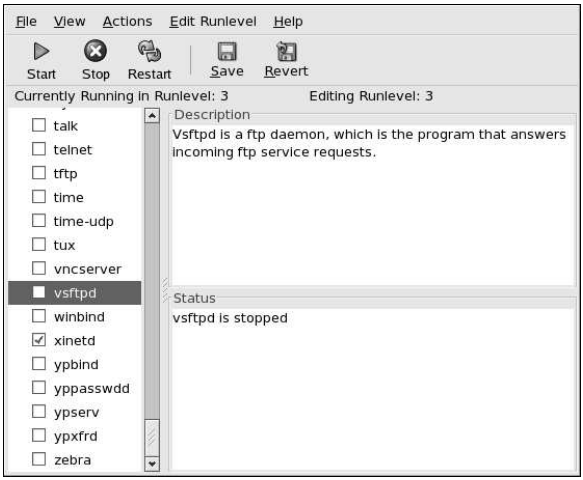

Abbildung 4-3. Services Configuration Tool

Wenn Sie sich nicht sicher sind, welchen Zweck ein Dienst hat, finden Sie im **Services Configuration Tool** ein Beschreibungsfeld, in Abbildung 4-3 abgebildet, das Ihnen von Nutzen sein kann.

Das reine Überprüfen, welche Netzwerkdienste zum Bootzeitpunkt verfügbar sind, ist jedoch nicht genug. Kompetente Systemadministratoren sollten auch prüfen, welche Ports offen sind und eingehende Signale abhören. Weitere Informationen zu diesem Thema finden Sie unter Abschnitt 5.8.

4.5.3. Unsichere Dienste

Jeder Netzwerkdienst is potentiell unsicher. Aus diesem Grund ist es wichtig, nicht benötigte Dienste zu deaktivieren. Angriffsflächen für Dienste werden so erkannt und können gepatcht werden. Es ist daher wichtig, Pakete, die für einen Netzwerkdienst benötigt werden, auf dem neuesten Stand zu halten. Weitere Informationen hierzu finden Sie unter Kapitel 3.

Einige Netzwerkprotokolle sind von Natur aus unsicherer als andere. Dies umfasst Dienste, die wie folgt eingesetzt werden:

- *Unverschlüsselte Übertragung von Benutzernamen und Passwörtern über ein Netzwerk* — Viele ältere Protokolle, z.B. Telnet und FTP, verschlüsseln die Authentifizierung nicht, und sollten möglichst deaktiviert werden.
- *Emfpindliche Daten unverschlüsselt über ein Netzwerk versenden* — Viele Protokolle übertragen Daten unverschlüsselt über ein Netzwerk. Diese Protokolle sind unter anderem Telnet, FTP, HTTP und SMTP. Viele Netzwerk-Dateisysteme, z.B. NFS und SMB, übertragen auch Informationen unverschlüsselt über das Netzwerk. Es liegt in der Verantwortung des Benutzers, einzuschränken, welche Art Daten bei der Verwendung dieser Protokolle übertragen werden dürfen.

  Auch remote Speicherabbildungsdienste wie `netdump` übertragen den Inhalt eines Speichers unverschlüsselt über das Netzwerk. Memory Dumps können Passwörter, oder schlimmer noch, Datenbankeinträge und andere empfindliche Informationen enthalten.

  Andere Dienste wie `finger` und `rwhod` geben Informationen über Benutzer im System preis.

Beispiele für von Natur aus unsichere Dienste sind unter anderem folgende:

- `rlogin`
- `rsh`
- `telnet`
- `vsftpd`

Alle Remote-Login- und Shell-Programme (`rlogin`, `rsh` und `telnet`) sollten zugunsten von SSH vermieden werden. (Unter Abschnitt 4.7 finden Sie weitere Informationen zu `sshd`).

FTP ist nicht ganz so gefährlich für die Sicherheit des Systems wie Remote-Shells, FTP-Server müssen jedoch sorgfältig konfiguriert und überwacht werden, um Probleme zu vermeiden. Weitere Informationen über das Sichern von FTP-Servern finden Sie unter Abschnitt 5.6.

Dienste, die sorgfältig implementiert und hinter einer Firewall verwendet werden sollten, umfassen folgende:

- `finger`
- `identd`
- `netdump`
- `netdump-server`
- `nfs`
- `rwhod`
- `sendmail`
- `smb` (Samba)
- `yppasswdd`
- `ypserv`
- `ypxfrd`

Weitere Informationen zur Sicherung von Netzwerkdiensten ist unter Kapitel 5 erhältlich.

Im nächsten Abschnitt werden Tools für das Einrichten einer Firewall beschrieben.

4.6. Persönliche Firewalls

Sobald die *nötigen* Netzwerkdienste konfiguriert sind, ist es wichtig, eine Firewall zu implementieren.

Firewalls verhindern, dass Netzwerkpakete Zugriff auf die Netzwerkschnittstelle des Systems erhalten. Wird eine Anfrage an einen Port gestellt, der von einer Firewall geschützt ist, wird diese Anfrage ignoriert. Hört ein Dienst einen dieser blockierten Ports ab, kann dieser Dienst die Pakete nicht empfangen, und ist somit effektiv deaktiviert. Aus diesem Grund sollte man bei der Konfiguration einer Firewall darauf achten, dass der Zugang zu nicht benutzten Ports blockiert wird, Ports für konfigurierte Dienste jedoch offen bleiben.

Für die meisten Benutzer ist das beste Tool zur Konfiguration einer einfachen Firewall das einfache, grafische Firewall-Konfiguration-Tool, das mit Red Hat Enterprise Linux ausgeliefert wird: **Security Level Configuration Tool** (`system-config-securitylevel`). Dieses Tool erzeugt breite `iptables`-Regeln für eine allgemeine Firewall, unter Verwendung eines Control-Panel-Interface

Weitere Informationen über die Verwendung dieser Applikation und deren Optionen finden Sie im Kapitel *Basiskonfiguration der Firewall* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Für fortgeschrittene Benutzer und Server-Administratoren ist wahrscheinlich die beste Option das Konfigurieren einer Firewall von Hand mit dem Befehl `iptables`. Weitere Informationen finden Sie unter Kapitel 7. Einen umfassenden Leitfaden zum `iptables`-Befehl finden Sie im Kapitel *Firewalls und `iptables`* im *Red Hat Enterprise Linux Referenzhandbuch*.

4.7. Kommunikationstools mit erhöhter Sicherheit

Mit wachsender Verbreitung und Beliebtheit des Internets wächst auch die Bedrohung durch Abfangen von Kommunikation. In den letzten Jahren wurden Tools entwickelt, die jegliche Kommunikation bei der Übertragung über das Netzwerk verschlüsseln.

Red Hat Enterprise Linux wird mit zwei einfachen Tools geliefert, die hochrangige Verschlüsselungsalgorithmen, basierend auf öffentlichen Schlüsseln, verwenden, um Informationen während der Übertragung im Netzwerk zu schützen.

- *OpenSSH* — Eine frei-erhältliche Implementierung des SSH-Protokolls zur Verschlüsselung von Netzwerkkommunikation.
- *Gnu Privacy Guard (GPG)* — Eine frei-erhältliche Implementierung der PGP (Pretty Good Privacy) Verschlüsselungs-Applikation zur Verschlüsselung von Daten.

OpenSSH ist eine sichere Methode für den Zugang zur einer entfernten Maschine und ersetzt ältere, unverschlüsselte Dienste wie `telnet` und `rsh`. OpenSSH enthält einen Netzwerkdienst mit dem Namen `sshd` und drei Befehlszeilen-Client-Applikationen:

- `ssh` — Ein sicherer Zugangs-Client für Remote-Konsolen.
- `scp` — Ein sicherer Befehl für Remote-Copy.
- `sftp` — Ein sicherer Pseudo-FTP-Client, der interaktive Dateiübertragung ermöglicht.

Es wird dringend empfohlen, das jegliche Remote-Kommunikation in Linux-Systemen über das SSH-Protokoll abgewickelt werden. Weitere Informationen zu OpenSSH finden Sie im Kapitel *OpenSSH*

im *Red Hat Enterprise Linux Handbuch zur System-Administration*. Weitere Informationen über das SSH-Protokoll finden Sie im Kapitel *SSH-Protokoll* im *Red Hat Enterprise Linux Referenzhandbuch*.

Wichtig

Obwohl der `sshd`-Dienst von Natur aus unsicher ist, *muss* dieser Dienst auf dem neuesten Stand gehalten werden, um Sicherheitsgefährdungen zu vermeiden. Unter Kapitel 3 finden Sie weitere Informationen zu diesem Thema.

GPG ist eine sehr gute Methode, um private Daten privat zu halten. Es kann zum Versenden empfindlicher Daten über öffentliche Netzwerke und desweiteren zum Schutz empfindlicher Daten auf Festplatten eingesetzt werden.

Weitere Informationen zu GPG finden Sie im Anhang *Einführung in Gnu Privacy Guard* im*<Red Hat Enterprise Linux Schrittweise Einführung*.

Kapitel 5.

Server-Sicherheit

Wenn ein System als Server in einem öffentlichen Netzwerk verwendet wird, wird dieses zu einem Angriffsziel. Aus diesem Grund ist das Abhärten des Systems und Sperren von Diensten von erheblicher Bedeutung für den Systemadministrator.

Bevor Sie die Details eines bestimmten Themas erforschen, sehen Sie sich die folgenden allgemeinen Hinweise für das Erhöhen der Server-Sicherheit an:

- Halten Sie alle Dienste auf dem neuesten Stand, um vor den neuesten Bedrohungen geschützt zu sein.
- Verwenden Sie sichere Protokolle.
- Wenn möglich, sollte immer nur eine Maschine einen Netzwerkdienst bereitstellen.
- Überwachen Sie alle Server sorgfältig auf verdächtige Aktivitäten.

5.1. Sichern von Diensten mit TCP Wrappern und `xinetd`

TCP-Wrapper bieten Zugriffskontrolle für eine Reihe von Diensten. Die meisten modernen Netzwerkdienste, wie z.B. SSH, Telnet und FTP, verwenden TCP-Wrapper, die als Wachposten zwischen einer eingehenden Anfrage und dem angefragten Dienst stehen.

Die Vorteile von TCP Wrappern werden noch erweitert, wenn diese zusammen mit `xinetd`, einem Super-Dienst, der zusätzliche Zugriffs-, Log-, Bindungs-, Umleitungs- und Ressourcenkontrolle bietet.

Tipp

Es ist eine gute Idee, die IPTables-Firewall-Regeln in Zusammenhang mit TCP Wrappern und `xinetd` zu verwenden, um eine Redundanz innerhalb der Service-Zugangskontrollen zu erreichen. Für mehr Information über das Errichten von Firewalls mit IPTables-Befehlen sieheKapitel 7.

Weitere Informationen zur Konfiguration von TCP Wrappern und `xinetd` finden Sie im Kapitel *TCP Wrapper und* `xinetd` im *Red Hat Enterprise Linux Referenzhandbuch*.

In den folgenden Unterkapiteln wird davon ausgegangen, dass Sie ein grundlegendes Wissen über jedes Thema besitzen und sich auf spezielle Sicherheitsoptionen konzentrieren.

5.1.1. Erhöhung der Sicherheit mit TCP Wrappern

TCP Wrapper können viel mehr als nur Zugriffe auf Dienste verweigern. In diesem Abschnitt wird erläutert, wie TCP Wrapper zum Versenden von Verbindungs-Bannern, Warnen vor Angriffen von bestimmten Hosts und Erweitern der Log-Funktionalität eingesetzt werden können. Eine ausführliche Liste der Funktionalität und Kontrollsprache der TCP Wrapper finden Sie auf den man-Seiten der `hosts_options`.

5.1.1.1. TCP Wrapper und Verbindungs-Banner

Den mit einem Dienst verbundenen Clients ein einschüchterndes Banner zu schicken, ist eine gute Methode, um zu verschleiern, welches System der Server verwendet, und im gleichen Zug Angreifer wissen zu lassen, dass sie es mit einem wachsamen Systemadministrator zu tun haben. Um ein TCP-Wrapper Banner für einen Dienst zu implementieren, verwenden Sie die Option `banner`.

In diesem Beispiel wird ein Banner für `vsftpd` implementiert. Sie müssen zuerst eine Banner-Datei anlegen. Diese kann sich irgendwo auf dem System befinden, muss aber den gleichen Namen wie der Daemon haben. In diesem Beispiel nennen wir die Datei `/etc/banners/vsftpd`.

Der Inhalt der Datei sieht wie folgt aus:

```
220-Hello, %c
220-All activity on ftp.example.com is logged.
220-Act up and you will be banned.
```

Der `%c` Token liefert eine Reihe von Client-Informationen wie den Benutzernamen oder den Hostnamen, oder den Benutzernamen und die IP-Adresse, um die Verbindung einschüchternder zu machen. In *Red Hat Enterprise Linux Referenzhandbuch* finden Sie eine Liste mit anderen verfügbaren Tokens für TCP Wrapper.

Damit dieses Banner eingehenden Verbindungen präsentiert werden kann, fügen Sie die folgende Zeile in die Datei `/etc/hosts.allow` ein:

```
vsftpd : ALL : banners /etc/banners/
```

5.1.1.2. TCP Wrapper und Warnung vor Angriffen

Wenn ein bestimmter Host oder ein Netzwerk bei einem Angriff auf den Server ertappt wurde, können TCP Wrapper mit der `spawn`-Direktive vor weiteren Angriffen von diesem Host oder Netzwerk warnen.

In diesem Beispiel gehen wir davon aus, dass ein Cracker vom 206.182.68.0/24 Netzwerk bei einem Angriffsversuch auf den Server erwischt wurde. Indem Sie die folgende Zeile in die Datei `/etc/hosts.deny` einfügen, wird der Verbindungsversuch abgewiesen und in einer besonderen Datei aufgezeichnet:

```
ALL : 206.182.68.0 : spawn /bin/ 'date' %c %d >> /var/log/intruder_alert
```

Das `%d`-Token liefert den Namen des Dienstes, auf den der Angreifer zugreifen wollte.

Um die Verbindung zu erlauben und diese aufzuzeichnen, fügen Sie die `spawn` Direktive in die Datei `/etc/hosts.allow` ein.

Hinweis

Da die `spawn`-Direktive jeden beliebigen Shell-Befehl ausführt, können Sie ein spezielles Skript schreiben, das den Administrator im Falle eines Verbindungsversuchs eines bestimmten Clients mit dem Server benachrichtigt oder eine Reihe von Befehlen ausführt.

5.1.1.3. TCP Wrapper und erweitertes Logging

Wenn bestimmte Verbindungstypen eine größere Sorge darstellen als andere, kann der Log-Level für diesen Dienst über die Option `severity` angehoben werden.

In diesem Beispiel gehen wir davon aus, dass jeder, der eine Verbindung zu Port 23 (dem Telnet-Port) auf einem FTP-Server herstellen will, ein Cracker ist. Um dies zu kennzeichnen, fügen Sie eine `emerg`-Flag anstelle der Standard-Flag `info` in die Log-Datei ein und verweigern Sie die Verbindung.

Hierfür fügen Sie die folgende Zeile in die Datei `/etc/hosts.deny` ein:

```
in.telnetd : ALL : severity emerg
```

Dies verwendet die standardmäßige `authpriv` Logging-Funktion, jedoch wird die Priorität vom Standardwert `info` auf `emerg` hinaufgesetzt, wodurch Log-Nachrichten direkt an die Konsole weitergegeben werden.

5.1.2. Erhöhen der Sicherheit mit `xinetd`

Der `xinetd` Super-Server ist ein weiteres nützliches Tool zur Zugriffskontrolle auf die untergeordneten Server. In diesem Abschnitt wird beschrieben, wie `xinetd` eingesetzt werden kann, um einen sogenannten Trap-Service einzurichten und die Anzahl der Ressourcen, die zur Unterbindung von DoS-Angriffen in jedem beliebigen `xinetd`-Dienst zu Verfügung stehen, zu kontrollieren. Eine eingehendere Liste der verfügbaren Optionen finden Sie auf den man-Seiten zu `xinetd` und `xinetd.conf`.

5.1.2.1. Eine Falle aufstellen

Ein wichtiges Feature von `xinetd` ist die Fähigkeit, Hosts zu einer globalen `no_access`-Liste hinzufügen zu können. Den Hosts auf dieser Liste werden Verbindungen zu Diensten, die von `xinetd` verwaltet werden, für einen bestimmten Zeitraum oder bis `xinetd` neu gestartet wird, verweigert. Dies wird durch das `SENSOR`-Attribut erreicht. Durch diese Methode können Sie auf einfache Weise Hosts blockieren, die den Server auf offene Ports absuchen.

Der erste Schritt für das Einrichten des `SENSOR` ist, einen Dienst auszuwählen, den Sie nicht für eine Verwendung einplanen. In diesem Beispiel wird Telnet verwendet.

Bearbeiten Sie die Datei `/etc/xinetd.d/telnet` und ändern Sie die Zeile `flags` in folgendes um:

```
flags           = SENSOR
```

Fügen Sie die folgendes Zeile innerhalb der Klammern hinzu:

```
deny_time       = 30
```

Hierdurch wird dem Host, der 30 Minuten lang versucht hat, sich mit dem Port zu verbinden, der Zugriff verweigert. Andere Werte für das `deny_time`-Attribut sind FOREVER, der solange wirksam ist, bis `xinetd` neu gestartet wird, und NEVER, der die Verbindung zulässt und sie dokumentiert.

Die letzte Zeile sollte wie folgt aussehen:

```
disable         = no
```

Obwohl `SENSOR` eine gute Methode ist, Verbindungen von böswilligen Hosts zu erkennen und zu stoppen, hat es jedoch zwei Nachteile:

- Es hilft nicht gegen heimliches Scannen (Stealth Scans).

- Ein Angreifer, der weiß, dass ein `SENSOR` ausgeführt ist, kann eine DoS-Attacke gegen bestimmte Hosts ausführen, indem er ihre IP-Adressen fälscht und sich mit dem verbotenen Port verbindet.

5.1.2.2. Kontrollieren von Server-Ressourcen

Ein weiteres, wichtiges Feature von `xinetd` ist die Fähigkeit, die Anzahl der Ressourcen, die Dienste zur Verfügung haben, zu kontrollieren.

Dies wird durch die folgenden Direktiven erreicht:

- `cps = <number_of_connections> <wait_period>` — Gibt die Verbindungen pro Sekunde zu einem Service vor. Diese Direktive akzeptiert nur ganze Zahlen.
- `instances = <number_of_connections>` — Gibt die Gesamtzahl aller erlaubten Verbindungen zu einem Dienst an. Diese Direktive akzeptiert entweder ganze Zahlen oder `UNLIMITED`.
- `per_source = <number_of_connections>` — Gibt die Verbindungen zu einem Dienst pro Host vor. Diese Direktive akzeptiert entweder einen ganzzahligen Wert oder `UNLIMITED`.
- `rlimit_as = <number[K|M]>` — Gibt die Größe der Speicheradresse in Kilobyte oder Megabyte an, die der Dienst in Anspruch nehmen kann kann. Diese Direktive akzeptiert entweder einen ganzzahligen Wert oder `UNLIMITED`.
- `rlimit_cpu = <number_of_seconds>` — Gibt die Zeit in Sekunden an, die ein Dienst die CPU belegen kann. Diese Direktive akzeptiert entweder einen ganzzahligen Wert oder `UNLIMITED`.

Mithilfe dieser Direktiven kann verhindert werden, dass ein `xinetd`-Dienst das gesamte System belegt und Denial-of-Service verursacht.

5.2. Portmap sichern

Der `portmap`-Dienst ist ein dynamischer Port-Zuweisungs-Daemon für RPC-Dienste wie NIS und NFS. Es besitzt schwache Authentifizierungsmechanismen und hat die Fähigkeit, eine große Bandbreite an Ports für die von ihm kontrollierten Dienste zuzuweisen. Aus diesen Gründen ist portmap schwer zu sichern.

Hinweis

Das Sichern von `portmap` betrifft lediglich NFSv2 und NFSv3 Implementationen, da dies für NFSv4 nicht mehr länger erforderlich ist. Wenn Sie vorhaben, einen NFSv2 oder NFSv3 Server zu implemenieren, dann ist `portmap` erforderlich und der folgende Abschnitt findet Anwendung.

Wenn Sie RPC-Dienste ausführen, sollten Sie diese Grundregeln beachten.

5.2.1. Schützen von `portmap` mit TCP Wrappern

Es ist wichtig, TCP Wrapper zur Einschränkung des Zugriffs von Netzwerken und Hosts auf den `portmap`-Dienst einzusetzen, da letzterer keine integrierte Authentifizierungsmöglichkeit bietet.

Desweiteren sollten Sie *nur* IP-Adressen verwenden, wenn Sie den Zugriff auf den Dienst einschränken wollen. Vermeiden Sie Hostnamen, da sie durch DNS-Poisoning und andere Methoden gefälscht werden können.

5.2.2. Schützen von `portmap` mit IPTables

Um den Zugriff auf den `portmap`-Dienst weiter einzuschränken, ist es sinnvoll, IPTables-Regeln zum Server hinzuzufügen, die den Zugriff auf bestimmte Netzwerke einschränken.

Unten finden Sie zwei Beispiele für IPTables-Befehle, die TCP-Verbindungen zum `portmap`-Dienst (auf Port 111) vom 192.168.0/24 Netzwerk und vom Localhost (der für den `sgi_fam`-Dienst für **Nautilus** benötigt wird) ermöglichen. Alle anderen Pakete werden abgelehnt.

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24  --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1  --dport 111 -j ACCEPT
```

Um auf gleiche Weise UDP-Traffic einzuschränken, verwenden Sie den folgenden Befehl.

```
iptables -A INPUT -p udp -s! 192.168.0.0/24  --dport 111 -j DROP
```

Tipp

Unter Kapitel 7 finden Sie weitere Informationen zum Errichten von Firewalls mit dem IPTables-Befehl.

5.3. Sichern von NIS

NIS steht für Network Information Service. Es ist ein RPC-Dienst mit dem Namen `ypserv`, der zusammen mit `portmap` und anderen zugehörigen Diensten verwendet wird, um Informationen zu Benutzernamen, Passwörtern und anderen empfindlichen Daten an jeden beliebigen Computer innerhalb dessen Domain weiterzugeben.

Ein NIS-Server besteht aus mehreren Applikationen, unter anderem:

- `/usr/sbin/rpc.yppasswdd` — Auch `yppasswdd`-Dienst genannt. Dieser Daemon ermöglicht Benutzern, ihre NIS-Passwörter zu ändern.
- `/usr/sbin/rpc.ypxfrd` — Auch `ypxfrd`-Dienst genannt. Dieser Daemon ist für den NIS-Map-Transfer über das Netzwerk verantwortlich.
- `/usr/sbin/yppush` — Diese Applikation verbreitet geänderte NIS-Datenbanken an mehrere NIS-Server.
- `/usr/sbin/ypserv` — Dies ist der NIS-Server-Daemon.

Im Vergleich zu heutigen Standards ist NIS als eher unsicher einzustufen. Es besitzt keine Host-Authentifizierungsmechanismen und überträgt Informationen, einschließlich Passwort-Hashes, unverschlüsselt über das Netzwerk. Aus diesem Grund müssen Sie beim Einrichten eines Netzwerks mit NIS extreme Vorsicht walten lassen. Dadurch, dass die Standard-Konfiguration von NIS von Natur aus unsicher ist, wird die Angelegenheit noch weiter verkompliziert.

Es wird empfohlen, dass Sie, bevor Sie einen NIS-Server implementieren wollen, zuerst den `portmap`-Dienst wie unter Abschnitt 5.2 beschrieben sichern und dann weitere Angelegenheiten wie Netzwerkplanung angehen.

5.3.1. Planen Sie das Netzwerk sorgfältig

Da NIS empfindliche Informationen unverschlüsselt über das Netzwerk überträgt, ist es wichtig, dass dieser Dienst hinter eine Firewall und auf einem segmentierten und sicheren Netzwerk ausgeführt wird. Jedes Mal, wenn NIS-Informationen über ein unsicheres Netzwerk übertragen werden, wird das Abfangen von Daten riskiert. Hier kann ein sorgfältiges Design des Netzwerks schwerwiegende Sicherheitsbrüche verhindern.

5.3.2. Verwenden Sie Passwort-ähnliche NIS-Domainnamen und Hostnamen

Jede Maschine innerhalb einer NIS-Domain kann über bestimmte Befehle, ohne Authentifizierung, Informationen von einem Server extrahieren, solange der Benutzer den DNS-Hostnamen und den NIS-Domain-Namen des NIS-Servers kennt.

Wenn sich zum Beispiel jemand mit einem Laptop in das Netzwerk einklinkt oder von außen ins Netzwerk eindringt (und es schafft, eine interne IP-Adresse vorzutäuschen), enthüllt der folgende Befehl die `/etc/passwd`-Map:

```
ypcat -d <NIS_domain> -h <DNS_hostname> passwd
```

Ist der Angreifer ein Root-Benutzer, kann dieser die Datei `/etc/shadow` durch folgenden Befehl einsehen:

```
ypcat -d <NIS_domain> -h <DNS_hostname> shadow
```

Hinweis

Wenn Kerberos verwendet wird, wird die Datei `/etc/shadow` nicht innerhalb einer NIS-Map gespeichert.

Um den Zugang zu NIS-Maps für einen Angreifer zu erschweren, erstellen Sie einen zufälligen String für den DNS-Hostnamen, wie zum Beispiel `o7hfawtgmhwg.domain.com`. Erstellen Sie in gleicher Weise einen *anderen*, zufallsgenerierten NIS-Domain-Namen. Hierdurch wird es einem Angreifer erheblich erschwert, Zugang zum NIS-Server zu erhalten.

5.3.3. Bearbeiten Sie die Datei `/var/yp/securenets`

NIS hört alle Netzwerke ab, wenn die Datei `/var/yp/securenets` leer ist oder gar nicht existiert (dies ist z.B: nach einer Standard-Installation der Fall). Als erstes sollten Sie ein Netmask/Netzwerkpaar in der Datei hinterlegen, damit `ypserv` nur auf Anfragen des richtigen Netzwerks reagiert.

Unten finden Sie einen Beispieleintrag einer `/var/yp/securenets`-Datei:

```
255.255.255.0     192.168.0.0
```

Achtung

Sie sollten niemals einen NIS-Server zum ersten Mal starten, ohne vorher die Datei `/var/yp/securenets` erstellt zu haben.

Diese Methode schützt nicht vor einer IP-Spoofing-Attacke, schränkt jedoch die Netzwerke, die von NIS bedient werden, zumindest ein.

5.3.4. Zuweisung von Static Ports und Verwendung von IPTables -Regeln

Jedem der zu NIS gehörenden Server kann ein bestimmter Port zugewiesen werden, mit Ausnahme von `rpc.yppasswdd` — dem Daemon, der Benutzern das Ändern ihrer Login-Passwörter erlaubt. Indem Sie den anderen beiden NIS-Server-Daemons, `rpc.ypxfrd` und `ypserv`, Ports zuweisen, können Sie Firewall-Regeln erstellen, um die NIS-Server-Daemons noch mehr vor Eindringlingen zu schützen.

Hierzu fügen Sie die folgenden Zeilen zu `/etc/sysconfig/network` hinzu:

```
YPSERV_ARGS="-p 834"
YPXFRD_ARGS="-p 835"
```

Die folgenden IPTables-Regeln können erlassen werden, um festzulegen, welches Netzwerk der Server für diese Ports abhören soll:

```
iptables -A INPUT -p ALL -s! 192.168.0.0/24  --dport 834 -j DROP
iptables -A INPUT -p ALL -s! 192.168.0.0/24  --dport 835 -j DROP
```

Tipp

Unter Kapitel 7 finden Sie weitere Informationen zum Errichten von Firewalls mit dem IPTables-Befehl.

5.3.5. Verwenden Sie Kerberos-Authentifizierung

Einer der größten Mängel beim Verwenden von NIS für Authentifizierung ist, dass wenn sich ein Benutzer an einem Computer anmeldet, ein Passwort-Hash der `/etc/shadow`-Map über das Netzwerk verschickt wird. Wenn ein Angreifer Zugang zu einer NIS-Domain erhält und Verkehr über das Netzwerk durchschnüffelt, können Benutzernamen und Passwort-Hashes unbemerkt gesammelt werden. Mit genügend Zeit kann dann ein Passwort-Knack-Programm schwache Passwörter ermitteln und ein Angreifer kann dann auf einen gültigen Account im Netzwerk zugreifen.

Da Kerberos Verschlüsselungen mit geheimen Schlüsseln einsetzt, werden niemals Passwort-Hashes über das Netzwerk versandt, was das System erheblich sicherer macht. Weitere Informationen über Kerberos finden Sie im Kapitel *Kerberos* im *Red Hat Enterprise Linux Referenzhandbuch*.

5.4. Sicherung von NFS

Das *Network File System* oder *NFS* ist ein RPC-Dienst, der Client-Maschinen Dateisysteme, die vom Netzwerk aus zugängig sind, bereitstellt. Weitere Informationen zur Funktion von NFS finden Sie im Kapitel *Netzwerkdateisystem (NFS)* im *Red Hat Enterprise Linux Referenzhandbuch*. Weitere Informationen zur Konfiguration von NFS finden Sie im *Red Hat Enterprise Linux Handbuch zur System-Administration*. In den folgenden Unterabschnitten wird ein grundlegendes Wissen über NFS vorausgesetzt.

Wichtig

Die Version von NFS, die in Red Hat Enterprise Linux inkludiert ist, NFSv4, benötigt nicht mehr länger den `portmap`-Dienst, wie in Abschnitt 5.2 beschrieben. NFS-Verkehr benutzt nunmehr eher TCP in allen Versionen, als UDP und erfordert TCP unter Verwendung von NFSv4. NFSv4 beinhaltet nunmehr Kerberos Benutzer- und Gruppen-Authentifizierung als Teil des `RPCSEC_GSS` Kernel-Moduls. Informationen über `portmap` sind weiterhin beinhaltet, da Red Hat Enterprise Linux ebenso NFSv2 und NFSv3 unterstützt, welche `portmap` einsetzen.

5.4.1. Planen Sie das Netzwerk sorgfältig

Da nunmehr von NFSv4 sämtliche Informationen verschlüsselt mittels Kerberos über das Netzwerk übertragen werden können, ist es wichtig, dass dieser Dienst richtig konfiguriert wird, sollte sich dieser hinter einer Firewall oder auf einem segmentierten Netzwerk befinden. NFSv2 und NFSv3 übergeben Daten noch immer nicht sicher. Dabei besteht immer ein gewisser Grund zur Besorgnis. Hier kann ein sorgfältiges Design des Netzwerks schwerwiegende Sicherheitsbrüche verhindern.

5.4.2. Achtung vor Syntax-Fehlern

Der NFS-Server entscheidet über die Datei `/etc/exports`, welche Dateisysteme exportiert werden sollen und zu welchen Hosts diese Dateisysteme exportiert werden sollen. Achten Sie darauf, dass Sie keine Extra-Leerstellen beim Bearbeiten dieser Datei einfügen.

Die folgende Zeile in der Datei `/etc/exports` legt fest, dass der Host `bob.example.com` Lese- und Schreibberechtigung auf das gemeinsame Verzeichnis `/tmp/nfs/` erhält.

```
/tmp/nfs/     bob.example.com(rw)
```

Diese Zeile in der Datei `/etc/exports` beschreibt, dass der Host `bob.example.com` lediglich Leseberechtigung besitzt, allerdings *jeder* Lese- und Schreibberechtigung hat, wegen eines einzelnen Leerzeichens nach dem Hostnamen.

```
/tmp/nfs/     bob.example.com (rw)
```

Es ist sehr sinnvoll, jegliche konfigurierte NFS-Shares mit dem Befehl `showmount` zu prüfen:

```
showmount -e <hostname>
```

5.4.3. Verwenden Sie nicht die Option `no_root_squash`

Standardmäßig ändern NFS-Shares den Root-Benutzer in den Benutzer `nfsnobody` um, einem unprivilegierten Benutzer-Account. Auf diese Art gehören alle root-erstellten Dateien dem User `nfsnobody`, wodurch das Hochladen von Programmen mit der Setuid-Bit-Einstellung verhindert wird.

Wenn `no_root_squash` verwendet wird, können auswärtige Root-Benutzer jede Datei in dem gemeinsamen Dateisystem verändern und dabei trojanisierte Anwendungen hinterlassen, die von anderen Benutzern unabsichtlich ausgeführt werden.

5.5. Sicherung des Apache HTTP Server

Das Apache HTTP Server ist einer der stabilsten und sichersten Dienste, die mit Red Hat Enterprise Linux ausgeliefert werden. Es gibt eine unglaubliche Anzahl von Optionen und Methoden, um Apache HTTP Server — zu sichern, zu viele, um sie hier im Detail zu beschreiben.

Vor dem Konfigurieren von Apache HTTP Server sollten Sie die verfügbare Dokumentation für diese Applikation lesen. Dies umfasst das Kapitel *Apache HTTP Server* im *Red Hat Enterprise Linux Referenzhandbuch*, das Kapitel *Apache HTTP Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration* und die Handbücher zu Stronghold, verfügbar unter http://www.redhat.com/docs/manuals/stronghold/.

Unten finden Sie eine Liste mit Konfigurationsoptionen, die Administratoren nur mit Vorsicht verwenden sollten.

5.5.1. `FollowSymLinks`

Diese Direktive ist standardmäßig aktiviert, seien Sie also vorsichtig, wenn Sie symbolische Links zur Dokument-Root des Webservers erstellen. Es ist zum Beispiel keine gute Idee, einen symbolischen Link zu `/` zu setzen.

5.5.2. Die `Indexes` Direktive

Diese Direktive ist standardmäßig aktiviert, ist jedoch unter Umständen nicht wünschenswert. Wenn Sie nicht möchten, dass Benutzer Dateien auf dem Server durchsuchen, ist es sinnvoll, diese Direktive zu entfernen.

5.5.3. Die `UserDir` Direktive

Die `UserDir` Direktive ist standardmäßig deaktiviert, da sie das Bestehen eines Benutzeraccounts im System bestätigen kann. Wenn Sie das Browsen von Verzeichnissen auf dem Server durch Benutzer erlauben möchten, sollten Sie die folgenden Direktiven verwenden:

```
UserDir enabled
UserDir disabled root
```

Diese Direktiven aktivieren das Browsen von Verzeichnissen für alle Benutzer-Verzeichnisse außer `/root`. Wenn Sie Benutzer zu der Liste deaktivierter Accounts hinzufügen möchten, können Sie eine durch Leerstellen getrennte Liste der Benutzer in die Zeile `UserDir disabled` einfügen.

5.5.4. Entfernen Sie nicht die `IncludesNoExec`-Direktive

Standardmäßig kann das serverseitige Includes-Modul keine Befehle ausführen. Es wird davon abgeraten, diese Einstellungen zu ändern, außer wenn unbedingt notwendig, da dies einem Angreifer ermöglichen könnte, Befehle auf dem System auszuführen.

5.5.5. Schränken Sie Berechtigungen für ausführbare Verzeichnisse ein

Stellen Sie sicher, dass Sie Schreibberechtigungen für Verzeichnisse, die Skripte oder CGIs enthalten, nur für den Root-Benutzer vergeben. Dies erreichen Sie durch die folgenden Befehle:

```
chown root <directory_name>
chmod 755 <directory_name>
```

Prüfen Sie außerdem, dass jegliche Skripte, die Sie ausführen, auch wie beabsichtigt funktionieren, *bevor* sie in Produktion gegeben werden.

5.6. Sicherung von FTP

Das *File Transport Protocol* oder *FTP* ist ein älteres TCP-Protokoll, das zum Übertragen von Dateien über ein Netzwerk entwickelt wurde. Da alle Transaktionen mit dem Server, einschließlich der Benutzerauthentifizierung, unverschlüsselt ablaufen, wird es als ein unsicheres Protokoll betrachtet und sollte sorgfältig konfiguriert werden.

Red Hat Enterprise Linux bietet drei FTP-Server.

- `gssftpd` — Ein für Kerberos aktivierter, `xinetd`-basierter FTP-Daemon, der keine Authentifizierungsinformationen über das Netzwerk überträgt.
- **Red Hat Content Accelerator** (`tux`) — Ein Kernel-Space Webserver mit FTP Fähigkeiten.
- `vsftpd` — Eine einzelstehende, sicherheitsorientierte Implementierung des FTP-Dienstes.

Die folgenden Sicherheitsrichtlinien gelten für das Einrichten des `vsftpd`-FTP-Dienstes.

5.6.1. FTP-Grußbanner

Bevor der Benutzername und das Passwort eingereicht werden, erhalten alle Benutzer ein Grußbanner. Standardmäßig enthält dieses Banner Versionsinformationen, die für Cracker nützlich sein können, die Schwachstellen in einem System herausfinden wollen.

Um dieses Grußbanner für `vsftpd` zu ändern, fügen Sie die folgende Direktive zu `/etc/vsftpd/vsftpd.conf` hinzu:

```
ftpd_banner=<insert_greeting_here>
```

Ersetzen Sie *<insert_greeting_here>* in der obigen Direktive durch den Text Ihrer Begrüßung.

Für mehrzeilige Banner ist es ratsam, eine Bannerdatei zu verwenden. Um die Verwaltung von mehreren Bannern zu vereinfachen, speichern Sie alle Banner in einem neuen Verzeichnis mit dem Namen `/etc/banners/`. Die Bannerdatei für FTP-Verbindungen in diesem Beispiel ist `/etc/banners/ftp.msg`. Das untenstehende Beispiel zeigt, wie eine derartige Datei assehen kann:

```
#####################################################
# Hello, all activity on ftp.example.com is logged.#
#####################################################
```

Hinweis

Es ist nicht nötig, jede Zeile der Datei mit `220`, wie in Abschnitt 5.1.1.1 beschrieben, zu beginnen.

Um auf diese Grußbannerdatei für `vsftpd` zu referenzieren, fügen Sie folgende Direktive zu `/etc/vsftpd/vsftpd.conf` hinzu:

```
banner_file=/etc/banners/ftp.msg
```

Es ist auch möglich, zusätzliche Banner für eingehende Verbindungen mittels TCP Wrappern zu senden. Dies wird unter Abschnitt 5.1.1.1 beschrieben.

5.6.2. Anonymer Zugang

Das Vorhandensein des `/var/ftp/`-Verzeichnisses aktiviert das anonyme Account.

Der einfachste Weg, dieses Verzeichnis zu erstellen, ist durch die Installation des `vsftpd`-Pakets. Dieses Paket erstellt einen Verzeichnisbaum für anonyme Benutzer und vergibt anonymen Benutzern lediglich Lese-Berechtigungen für Verzeichnisse.

Standardmäßig können anonyme Benutzer nicht in Verzeichnisse schreiben.

Vorsicht

Wenn Sie einen anonymen Zugang zu FTP-Servern zulassen, sollten Sie darauf achten, wo Sie empfindliche Daten speichern.

5.6.2.1. Anonymes Hochladen

Wenn Sie anonymen Benutzern erlauben möchten, Dateien hochzuladen, wird empfohlen, ein Verzeichnis nur mit Schreibberechtigung innerhalb von `/var/ftp/pub/` anzulegen.

Hierfür geben Sie folgendes ein:

```
mkdir /var/ftp/pub/upload
```

Ändern Sie dann wie folgt die Berechtigungen, so dass anonyme Benutzer nicht sehen können, was sich innerhalb des Verzeichnisses befindet:

```
chmod 730 /var/ftp/pub/upload
```

Eine detaillierte Auflistung des Verzeichnisses sollte wie folgt aussehen:

```
drwx-wx---    2 root     ftp          4096 Feb 13 20:05 upload
```

Achtung

Administratoren, die anonymen Benutzern Lese- und Schreibberechtigungen für Verzeichnisse geben, stellen häufig fest, dass ihr Server dann zu einer Fundgrube gestohlener Software wird.

Fügen Sie zusätzlich unter `vsftpd` die folgende Zeile in die Datei `/etc/vsftpd/vsftpd.conf` ein:

```
anon_upload_enable=YES
```

5.6.3. Benutzeraccounts

Da FTP unverschlüsselt Benutzernamen und Passwörter über unsichere Netzwerke zur Authentifizierung überträgt, ist es ratsam, Systembenutzerzugang zum Server von den Benutzeraccounts aus zu verbieten.

Um Benutzeraccounts in `vsftpd` zu deaktivieren, fügen Sie die folgende Direktive zu `/etc/vsftpd/vsftpd.conf` hinzu:

```
local_enable=NO
```

5.6.3.1. Benutzeraccounts einschränken

Der einfachste Weg, eine bestimmte Gruppe von Accounts, wie den Root-Benutzer und solche mit `sudo`-Berechtigungen, am Zugriff auf den FTP-Server zu hindern, ist durch eine PAM-Liste, wie unter Abschnitt 4.4.2.4 beschrieben. Die PAM-Konfigurationsdatei für `vsftpd` ist `/etc/pam.d/vsftpd`.

Es ist auch möglich, Benutzeraccounts innerhalb jeden Dienstes direkt zu deaktivieren.

Um bestimmte Benutzeraccounts in `vsftpd` zu deaktivieren, fügen Sie den Benutzernamen zu `/etc/vsftpd.ftpusers` hinzu.

5.6.4. TCP Wrapper für die Zugriffskontrolle

Sie können TCP Wrapper für die Zugriffskontrolle zu den FTP-Daemons wie unter Abschnitt 5.1.1 beschrieben einsetzen.

5.7. Sicherung von Sendmail

Sendmail ist ein Mail Transport Agent (MTA), der das Simple Mail Transport Protocol (SMTP) zur Übertragung elektronischer Nachrichten zwischen anderen MTAs und für das E-Mailen an Clients oder Delivery Agents einsetzt. Obwohl viele MTAs den Verkehr untereinander verschlüsseln können, tun dies viele nicht, so dass das Versenden von E-Mails über ein öffentliches Netzwerk als eine von Natur aus unsichere Form der Kommunikation betrachtet wird.

Weitere Informationen zur Funktionsweise von E-Mails und einen Überblick allgemeiner Konfigurationseinstellungen finden Sie im Kapitel *E-Mail* im *Red Hat Enterprise Linux Referenzhandbuch*. Dieser Abschnitt setzt ein Grundwissen über das Generieren einer gültigen `/etc/mail/sendmail.cf` durch das Bearbeiten von `/etc/mail/sendmail.mc` und dasAusführen des Befehls `m4` voraus. Dies wird im *Red Hat Enterprise Linux Referenzhandbuch* beschrieben.

Es wird empfohlen, dass Sie sich mit den folgenden Angelegenheiten auseinandersetzen, wenn Sie die Implementierung eines Sendmail-Servers planen.

5.7.1. Limitierung einer Denial-of-Service-Attacke

Durch die Natur von E-Mail kann ein dazu entschlossener Angreifer den Server leicht mit E-Mails überfluten und so eine Verweigerung des Dienstes verursachen. Indem Sie in die folgenden Direktiven in `/etc/mail/sendmail.mc` limitieren, kann die Wirksamkeit solcher Attacken stark abgeschwächt werden.

- `confCONNECTION_RATE_THROTTLE` — Die Anzahl der Verbindungen, die der Server pro Sekunde empfangen kann. Standardmäßig begrenzt Sendmail die Zahl der Verbindungen nicht. Wird eine Grenze gesetzt, werden darüber hinaus gehende Verbindungen verzögert.

- `confMAX_DAEMON_CHILDREN` — Die maximale Anzahl von Child-Prozessen, die vom Server erzeugt werden können. Standardmäßig begrenzt Sendmail die Anzahl der Child-Prozesse nicht. Wird eine Grenze gesetzt und diese erreicht, werden alle weiteren Verbindungen verzögert.
- `confMIN_FREE_BLOCKS` — Die minimale Anzahl freier Blöcke, die für den Server zur Verfügung stehen müssen, um E-Mail empfangen zu können. Der Standard ist 100 Blöcke.
- `confMAX_HEADERS_LENGTH` — Die maximal akzeptierte Größe (in Bytes) für einen Nachrichtenkopf.
- `confMAX_MESSAGE_SIZE` — Die maximal akzeptierte Größe (in Bytes) pro Nachricht.

5.7.2. NFS und Sendmail

Legen Sie niemals das Mail-Spool-Verzeichnis, `/var/spool/mail/`, auf einem NFS-Shared Volumen ab.

Da NFSv2 und NFSv3 keine Kontrolle über Benutzer- und Gruppen-IDs haben, können zwei oder mehr Benutzer die gleiche UID besitzen und daher jeweils die E-Mail des anderen lesen. Mit NFSv4 und Kerberos ist dies nicht der Fall, da das `SECRPC_GSS`-Kernel-Modul keine UID-basierte Authentifizierung anwendet.

5.7.3. Nur-Mail Benutzer

Um ein Ausbeuten des Sendmail-Servers durch lokale Benutzer zu vermeiden, ist es am besten, wenn Mail-Benutzer auf den Sendmail-Server nur über ein E-Mail-Programm zugreifen. Shell-Accounts auf dem Mail-Server sollten nicht erlaubt sein, und alle Benutzer-Shells in der Datei `/etc/passwd` sollten auf `/sbin/nologin` gesetzt sein (evtl. unter Ausnahme des Root-Benutzers).

5.8. Bestätigen, welche Ports auf Verbindungen abhören

Nachdem Sie die Netzwerk-Dienste konfiguriert haben, ist es wichtig, zu überprüfen, welche Ports die Netzwerkschnittstellen im System tatsächlich abhören. Alle offenen Ports können Beweis für ein unbefugtes Eindringen sein.

Es gibt zwei grundlegende Herangehensweisen für das Auflisten der Ports, die das Netzwerk abhören. Die weniger zuverlässige Methode ist, den Netzwerkstack durch Befehle wie `netstat -an` oder `lsof -i` abzufragen. Diese Methode ist daher unzuverlässiger, da die Programme sich nicht vom Netzwerk aus mit dem Computer verbinden, sondern eher prüfen, was auf dem System ausgeführt wird. Aus diesen Grund sind diese Applikationen häufig Ziel für Ersetzungen durch Angreifer. Durch diese Methode versuchen Cracker ihre Spuren zu verwischen, wenn diese unbefugt Netzwerkports geöffnet haben.

Ein etwas zuverlässigerer Weg für das Prüfen, welche Ports das Netzwerk abhören, ist mit einem Port-Scanner wie z.B. `nmap`.

Der folgende Befehl, von einer Konsole aus eingegeben, stellt fest, welche Ports auf TCP-Verbindungen aus dem Netzwerk mithören.

```
nmap -sT -O localhost
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-24 13:49 EDT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
113/tcp   open  auth
631/tcp   open  ipp
834/tcp   open  unknown
2601/tcp  open  zebra
32774/tcp open  sometimes-rpc11
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 12.857 days (since Sat Sep 11 17:16:20 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 5.190 seconds
```

Diese Ausgabe zeigt, dass das System `portmap` ausführt, dadurch, dass der Dienst `sunrpc` vorhanden ist. Es wird jedoch auch ein unbekannter Dienst auf Port 834 ausgeführt. Um zu prüfen, ob dieser Port zu der offiziellen Liste bekannter Dienste gehört, geben Sie folgendes ein:

```
cat /etc/services | grep 834
```

Dieser Befehl erhält keine Ausgabe. Dies bedeutet, dass der Port im reservierten Bereich (0 bis 1023) liegt und Root-Zugang zum Öffnen benötigt, jedoch nicht mit einem bekannten Dienste assoziiert ist.

Als nächstes können Sie Informationen über den Port mittels `netstat` oder `lsof` abrufen. Um Port 834 mit Hilfe von`netstat` zu prüfen, geben Sie folgenden Befehl ein:

```
netstat -anp | grep 834
```

Dieser Befehl erhält folgende Ausgabe:

```
tcp   0    0 0.0.0.0:834     0.0.0.0:*   LISTEN   653/ypbind
```

Das Vorhandensein eines offenen Ports in `netstat` ist beruhigend, da ein Cracker, der einen Port heimlich auf einem geknackten System öffnet, das Anzeigen des Ports durch diesen Befehl höchstwahrscheinlich nicht zulassen würde. Desweiteren zeigt die Option `[p]` die Prozess-ID (PID) des Dienstes an, der diesen Port geöffnet hat. In diesem Fall gehört der offene Port zu `ypbind` (NIS), ein RPC-Dienst, der zusammen mit dem `portmap`-Dienst abläuft.

Der `lsof`-Befehl zeigt ähnliche Informationen an, da auch hiermit offene Ports mit Diensten verknüpft werden:

```
lsof -i | grep 834
```

Unten finden Sie den betreffenden Teil der Ausgabe für diesen Befehl:

```
ypbind      653        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      655        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      656        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      657        0    7u  IPv4       1319                TCP *:834 (LISTEN)
```

Wie Sie sehen, können diese Tools eine Menge Informationen über den Status von Diensten auf einem Computer geben. Diese Tools sind flexibel und liefern eine Vielzahl von Informationen zu den Netzwerkdiensten und zur Konfiguration. Es wird deswegen dringend empfohlen, die man-Seiten zu `lsof`, `netstat`, `nmap` und `services` zu lesen.

Kapitel 6.

Virtuelle Private Netzwerke

Unternehmen mit mehreren Zweigstellen sind häufig über spezielle Leitungen miteinander verbunden, um Effizienz und Schutz empfindlicher Daten zu gewähren. Viele Firmen nutzen zum Beispiel Frame Relay oder *Asynchronous Transfer Mode* (ATM) Leitungen als End-to-End Netzwerklösung, um Büros miteinander zu verbinden. Dies kann eine teurere Lösung darstellen, insbesondere für kleine bis mittlere Unternehmen, die sich vergrößern, jedoch nicht die hohen Kosten für hochrangige Digitalschaltungen in Kauf nehmen wollen.

Virtuelle Private Netzwerke (VPN) stellen eine Lösung für dieses Problem dar. Dem Prinzip besonders zugewiesener Digitalschaltungen folgend, ermöglichen VPNs gesicherte, digitale Kommunikation zwischen zwei Parteien (oder Netzwerken) und erstellen somit ein Wide-Area-Netzwerk (WAN) aus bestehenden *Local-Area-Netzwerken* (LANs). Der Unterschied zum Frame Relay oder ATM ist das Transportmedium. VPNs übertragen über IP- oder Datagram (UDP)-Schichten, und sorgen somit für einen sicheren Transfer durch das Internet zum Bestimmungsort. Die meisten frei verfügbaren VPN-Implementierungen enthalten Open Standard, eine Open Source Verschlüsselung für das Maskieren von Daten während der Übertragung.

Einige Unternehmen setzen VPN-Hardwarelösungen ein, um die Sicherheit zu erhöhen, während andere Software- oder Protokoll-basierte Implementierungen verwenden. Es gibt mehrere Hersteller für Hardware-VPN-Lösungen, wie z.B. Cisco, Nortel, IBM und Checkpoint. Es gibt eine kostenlose, Software-basierte VPN-Lösung für Linux mit dem Namen FreeS/Wan, die eine standardisierte *IPSec* (Internet Protocol Security) Implementierung verwendet. Diese VPN-Lösungen verhalten sich wie spezielle Router, die sich in der IP-Verbindung von einem Büro zum nächsten befinden.

Wird ein Paket von einem Client übertragen wird, wird dies durch den Router oder das Gateway geschickt, die wiederum Header-Informationen für Routing und Authentifizierung hinzufügen, die *Authentication Header* (AH) genannt werden. Die Daten sind verschlüsselt und mit Anleitungen zur Entschlüsselung und Handhabung versehen, die *Encapsulating Security Payload* (ESP) genannt werden. Der empfangende VPN-Router holt sich die Header-Information und leitet diese zum Zielort weiter (entweder zu einer Workstation oder einem Knoten im Netzwerk). Unter Verwendung einer Netzwerk-zu-Netzwerk Verbindung erhält der empfangende Knoten am lokalen Netzwerk die Pakete unverschlüsselt und bereit zur Verarbeitung. Der Verschlüsselungs-/Entschlüsselungsprozess in einer Netzwerk-zu-Netzwerk VPN-Verbindung, ist für den lokalen Knoten transparent.

Durch solch einen erhöhten Grad an Sicherheit muss ein Cracker nicht nur ein Paket abfangen, sondern dies auch entschlüsseln. Eindringlinge, die eine Man-in-the-Middle-Attacke zwischen einem Server und einem Client durchführen, müssen daher auch Zugang zu mindestens einem der Schlüssel besitzen, die für die Authentifizierung verwendet werden. VPNs sind ein sicheres und effektives Mittel für die Verbindung mehrerer entfernter Knoten, die sich dann als ein vereinheitlichtes Intranet verhalten.

6.1. VPNs und Red Hat Enterprise Linux

Red Hat Enterprise Linux Benutzern stehen verschiedene Optionen in Hinsicht der Implementation einer Softwarelösung, um sich sicher mit derem WAN verbinden zu können. *Internet Protocol Security* oder IPsec ist die unterstützte VPN-Implementation für Red Hat Enterprise Linux, welches ausreichend den Nutzungsanforderungen von Organisationen mit Zweigstellen oder Remote-Benutzern gerecht wird.

6.2. IPsec

Red Hat Enterprise Linux unterstützt ein Protokoll zur gemeinsamen Verbindung von Remote-Hosts und Netzwerken, das einen sicheren Tunnel auf einem öffentlichen Netzwerk, wie dem Internet, verwendet. Das Protokoll, IPsec genannt, kann unter Verwendung einer Host-zu-Host (eine Workstation zu einer anderen) oder Netzwerk-zu-Netzwerk (eine LAN/WAN zu einem anderen) Verbindung implementiert werden. Die IPsec-Implementation in Red Hat Enterprise Linux benutzt Internet Key Exchange (*IKE*), das ein von Internet Engineering Task Force (IETF) implementiertes Protokoll darstellt. Es ist für beiderseitige Authentifizierung und sichere Verbindungen zwischen Systemen bestimmt.

Eine IPsec-Verbindung wird in zwei logische Phasen unterteilt. In Phase 1 initialisiert ein IPsec-Knoten die Verbindung mit dem Remote-Knoten oder -Netzwerk. Der Remote-Knoten oder das Remote-Netzwerk überprüft die Attribute (Credentials) des anfragenden Knotens und beide Parteien entscheiden über die Authentifizierungsmethode für die Verbindung. Auf Red Hat Enterprise Linux-Systemen benutzt eine IPsec-Verbindung die *Pre-shared Key*-Methode der IPsec Knoten-Authentifizierung. In dieser Art von Verbindung müssen beide Hosts den selben Schlüssel verwenden, um in die 2. Phase des IPsec-Verbindungsprozesses zu gelangen.

Phase 2 der IPsec-Verbindung ist diejenige, in der *Security Association* (SA) zwischen den IPsec-Knoten geschaffen wird. Diese Phase errichtet eine SA-Datenbank mit Konfigurationsinformationen, wie z.B. die Verschlüsselungsmethode, Secret-Session-Key (temporärer Schlüssel, den nur 2 Instanzen kennen) Austauschparameter und vieles mehr. In dieser Phase findet die eigentliche IPsec-Verbindung zwischen den entfernten Knoten und Netzwerken statt.

Die Red Hat Enterprise Linux Implementierung von IPsec verwendet IKE, damit die Schlüssel von den Hosts im ganzen Internet gemeinsam verwendet werden können. Der `racoon` Schlüssel-Deamon übernimmt die IKE-Schlüsselvergabe und den Austausch.

6.3. Installation von IPsec

Die Implementierung von IPsec erfordert, dass das `ipsec-tools` RPM-Paket auf allen IPsec-Hosts (wenn eine Host-zu-Host-Konfiguration verwendet wird) oder Routern (wenn eine Netzwerk-zu-Netzwerk-Konfiguration verwendet wird) installiert wird. Das RPM-Paket enthält essentielle Bibliotheken, Deamons und Konfigurationsdateien, die bei der Einrichtung der IPsec-Verbindung helfen.

- `/lib/libipsec.so` — Bibliothek, die die PF_KEY Trusted Key Management Socket Schnittstelle zwischen dem Linux-Kernel und der IPsec Implementierung enthält, die in Red Hat Enterprise Linux verwendet wird.
- `/sbin/setkey` — verändert das Schlüsselmanagement und die Sicherheitsattribute von IPsec im Kernel. Dieser Befehl wird vom `racoon` Schlüsselmanagement-Daemon kontrolliert. Für weitere Informationen über `setkey`, siehe `setkey`(8) man-Seite.
- `/sbin/racoon` — der IKE-Schlüsselmanagement- Daemon, der dazu verwendet wird, die Sicherheitszusammenhänge und das gemeinsame Verwenden von Schlüsseln zwischen IPsec-verbundenen Systemen zu leiten und zu kontrollieren. Dieser Daemon kann konfiguriert werden, indem die`/etc/racoon/racoon.conf` Datei bearbeitet wird.Für weitere Informationen über `racoon`, siehe `racoon`(8) man-Seite.
- `/etc/racoon/racoon.conf` — die `racoon` Daemon-Konfigurationsdatei, die verwendet wird, um verschiedene Bereiche der IPsec-Verbindung zu konfigurieren. Enthalten sind auch Methoden der Authentifizierung und Algorythmen zur Verschlüsselung, die bei der Verbindung verwendet werden. Eine komplette Liste der vorhandenen Direktiven finden Sie unter `racoon.conf`(5) man-Seite.

Die Konfiguration von IPsec auf Red Hat Enterprise Linux kann über das **Network Administration Tool** gemacht werden, oder durch manuelle Bearbeitung der Konfigurationen von Networking und

IPsec. Weitere Informationen über die Verwendung von **Network Administration Tool** siehe *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Wenn Sie zwei Netzwerk-verbundene Hosts über IPsec verbinden wollen, siehe Abschnitt 6.4. Um einen LAN/WAN mit einem anderen über IPsec zu verbinden, siehe Abschnitt 6.5.

6.4. Konfiguration von IPsec Host-zu-Host

Sie können IPsec so konfigurieren, dass ein Desktop oder eine Workstation mit einem(r) anderen über eine Host-zu-Host-Verbindung verbunden werden kann. Diese Art der Verbindung verwendet das Netzwerk, mit dem jeder Host verbunden ist, um einen sicheren Tunnel zueinander zu schaffen. Die Erfordernisse für eine Host-zu-Host-Verbindung sind minimal, wie auch die Konfiguration von IPsec bei jedem Host. Die Hosts brauchen lediglich eine bestimmte Verbindung zu einem Träger-Netzwerk (wie das Internet) und Red Hat Enterprise Linux um die IPsec-Verbindung herzustellen.

Der erste Schritt bei der Erstellung einer Verbindung ist das Einholen von System- und Netzwerk-informationen von jeder Workstation. Für eine Host- zu Host-Verbindung brauchen Sie die folgende Information:

- Die IP-Adressen für beide Hosts
- Einen einmaligen Namen, um die IPsec-Verbindung zu identifizieren und sie von anderen Geräten oder Verbindungen zu unterscheiden (z.B. `ipsec0`).
- Einen fixen Schlüssel zur Verschlüsselung oder einen, der automatisch von `racoon` geschaffen wurde.
- Ein bereits vorher gemeinsam verwendeter Schlüssel zu Authentifikation, der verwendet wird, um die Verbindung zu initialisieren und den Austausch von Schlüsseln zur Verschlüsselung möglich zu machen.

Stellen Sie sich z.B. vor, Workstation A und Workstation B wollen sich durch einen IPsec-Tunnel miteinander verbinden. Sie wollen sich unter Verwendung eines vorher gemeinsam verwendeten Schlüssels mit dem Wert von `foobarbaz`. Die Benutzer kommen überein, `racoon` automatisch einen Schlüssel zur Authentifikation generieren zu lassen, der von beiden Hosts gemeinsam verwendet wird. Beide Hosts entscheiden sich dafür, ihre Verbindungen `ipsec0` zu nennen.

Im folgenden sehen Sie die Datei `ifcfg` für Workstation A für eine Host-zu-Host-IPsec-Verbindung mit Workstation B. Der einmalige Name zur Identifizierung der Verbindung in diesem Beispiel ist *`ipsec0`*, der daraus resultierende Dateiname ist daher `/etc/sysconfig/network-scripts/ifcfg-ipsec0`:

```
DST=X.X.X.X
TYPE=IPSEC
ONBOOT=yes
IKE_METHOD=PSK
```

Workstation A würde *`X.X.X.X`* mit der IP Adresse von Workstation B ersetzen, während Workstation B *`X.X.X.X`* mit der IP Adresse von Workstation A ersetzen würde. Die Verbindung ist so eingestellt, dass sie beim Hochfahren startet (`ONBOOT=yes`) und verwendet die Authentifizierungs-Methode der vorher gemeinsam verwendeten Schlüssel (`IKE_METHOD=PSK`).

Im folgenden finden Sie die Datei mit den vorher gemeinsam benützten Schlüsseln (`/etc/sysconfig/network-scripts/keys-ipsec0` genannt), die beide Workstations verwenden, um sich gegenseitig zu authentifizieren. Der Inhalt dieser Datei sollte auf beiden Workstations identisch sein und nur der root-Benutzer sollte die Datei lesen oder überschreiben können.

```
IKE_PSK=foobarbaz
```

Wichtig

Um die `keys-ipsec0` Datei zu verändern, damit sie lediglich vom root-Benutzer gelesen oder bearbeitet werden kann, führen Sie nach der Erstellung der Datei den folgenden Befehl aus:

```
chmod 600 /etc/sysconfig/network-scripts/keys-ipsec0
```

Sie können den Authentifikations-Schlüssel jederzeit ändern. Bearbeiten Sie die `keys-ipsec0` Datei auf beiden Workstations. *Für eine ordentliche Verbindung müssen beide Schlüssel identisch sein* .

Im folgenden Beispiel sehen Sie die Konfigurationsdatei für die Verbindung zum Remote-Netzwerk. Die Datei trägt den Namen *X.X.X.X*`.conf` (ersetzen Sie *X.X.X.X* mit der IP Adresse des Remote-IPsec-Routers). Beachten Sie, dass diese Datei automatisch erzeugt wird, wenn der IPsec-Tunnel aktiviert wird und sollte nicht direkt bearbeitet werden.

```
;
remote X.X.X.X
{
        exchange_mode aggressive, main;
        my_identifier address;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2 ;
        }
}
```

Die Standardkonfigurationsdatei der Phase 1, die erzeugt wird, wenn eine IPsec-Verbindung initialisiert wird, beinhaltet folgenden Statements, die von der Red Hat Enterprise Linux-Implementierung von IPsec verwendet werden:

`remote` *X.X.X.X*

Legt fest, dass die nachfolgenden Stanzen dieser Konfigurationsdatei nur auf den entfernten Knoten zutreffen, der durch die IP-Adresse *X.X.X.X* identifiziert wird.

`exchange_mode aggressive`

Die Standardkonfiguration für IPsec auf Red Hat Enterprise Linux benutzt einen sog. aggressiven Authentifizierungsmodus, welcher den Overhead bei der Verbindung senkt, während gleichzeitig die Konfiguration von mehreren IPsec-Verbindungen mit mehrfachen Host ermöglicht wird.

`my_identifier address`

Legt die Identifikationsmethode fest, die bei der Authentifizierung von Knoten benutzt wird. Red Hat Enterprise Linux benutzt IP-Adressen, um Knoten zu identifizieren.

`encryption_algorithm 3des`

Legt den Verschlüsselungscode fest, der während der Authentifizierung benutzt wird. Standardmäßig wird *Triple Data Encryption Standard* (3DES) benutzt.

`hash_algorithm sha1;`

Legt den Hash-Algorithmus fest, der während der sogenannten Negotiation der Phase 1 zwischen den Knoten eingesetzt wird. Secure-Hash-Algorithmus Version 1 ist Standard.

`authentication_method pre_shared_key`

Legt die Authentifizierungsmethode fest, die während der Knoten-Negotiation benutzt wird. Red Hat Enterprise Linux benutzt standardmäßig 'vorinstallierte' Schlüssel (pre-shared Keys) zur Authentifizierung.

`dh_group 2`

Legt die Diffie-Hellman Gruppennummer zur Erstellung dynamisch generierter temporärer Schlüssel (Session Keys). Standardmäßig wird die 1024-Bit Gruppe benutzt.

Die `/etc/racoon/racoon.conf` Datei sollte auf allen IPsec-Knoten identisch sein, *bis auf* das `include "/etc/racoon/X.X.X.X.conf"`-Statement. Dieses Statement (und die Datei, auf die es sich bezieht) wird erstellt, wenn der IPsec-Tunnel aktiviert ist. Für Workstation A ist `X.X.X.X` im `include`-Statement die IP Adresse von Workstation B. Das Gegenteil gilt für Workstation B. Im Folgenden sehen Sie eine typische `racoon.conf`-Datei, wenn die IPsec Verbindung aktiviert ist.

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

sainfo anonymous
{
 pfs_group 2;
 lifetime time 1 hour ;
 encryption_algorithm 3des, blowfish 448, rijndael ;
 authentication_algorithm hmac_sha1, hmac_md5 ;
 compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf"
```

Diese standardmäßige `racoon.conf`-Datei beinhaltet festgelegte Pfade für die IPsec-Konfiguration, Dateien 'vorinstallierter' Schlüssel und Zertifikate. Die Felder in `sainfo anonymous` beschreiben die Phase 2 SA (Security Association) zwischen den IPsec-Knoten — die Natur der IPsec-Verbindung (inklusive den unterstützten Verschlüsselungs-Algorithmen, die Verwendung finden) und die Methode des Austauschens der Schlüssel. Die folgende Liste bestimmt die Felder der Phase 2:

`sainfo anonymous`

Bedeutet, dass SA mit jedem Peer anonym initialisieren kann, insofern die IPsec-Attribute (Credentials) übereinstimmen.

`pfs_group 2`

Legt das Diffie-Hellmann Schlüsselaustauschprotokoll fest, welches die Methode bestimmt, in der die IPsec-Knoten einen beiderseitigen, temporären Sitzungsschlüssel für die Verbindungsfähigkeit von IPsec in der 2. Phase einrichten. Standardmäßig benutzt die Red Hat Enterprise Linux-Implementierung von IPsec Gruppe 2 (oder `modp1024`) der Diffie-Hellmann kryptographischen Schlüsselaustausch-Gruppen. Gruppe 2 benutzt eine 1024-Bit modulare Exponentiation, welche Eindringlinge davon abhalten soll, bisherige IPsec-Übertragungen zu entschlüsseln, auch wenn ein privater Schlüssel dadurch gefährdet wird.

`lifetime time 1 hour`

Dieser Parameter legt den Lebenszuklus einer AS fest und kann entweder durch Zeit oder durch Datenmengen (Bytes) quantitativ bestimmt werden. Die Red Hat Enterprise Linux-Implementierung von IPsec legt eine einstündige Lebensdauer fest.

`encryption_algorithm 3des, blowfish 448, rijndael`

Legt den unterstützten Verschlüsselungscode für Phase 2 fest. Red Hat Enterprise Linux unterstützt 3DES, 448-Bit Blowfish und Rijndael (verwendet im *Advanced Encryption Standard* oder AES).

`authentication_algorithm hmac_sha1, hmac_md5`

Listet die unterstützten Hash-Algorithmen für Authentifizierung. Unterstützte Modi sind sha1 und md5 Hashed Message Authentication Codes (HMAC).

`compression_algorithm deflate`

Legt den Deflate-Compression-Algorithmus für IP-Payload Compression (IPCOMP) Unterstützung fest, was möglicherweise eine schnellere Übertragung von IP-Datagrammen über langsame Verbindungen ermöglicht.

Um die Verbindung zu starten, starten Sie entweder die Workstation neu oder führen Sie den folgenden Befehl als root auf jedem Host aus:

```
/sbin/ifup ipsec0
```

Um die IPsec-Verbindung zu testen, führen Sie die`tcpdump` Utility aus. Sie können so die Netzwerk-Pakete sehen, die zwischen den Hosts (oder den Netzwerken) übermittelt werden, und außerdem nachprüfen, dass sie über IPsec verschlüsselt weren. Jedes Paket sollte eine AH-Kopfzeile einhalten und als ESP-Paket angezeigt werden. EHP bedeutet, dass es verschlüsselt ist. Zum Beispiel:

```
17:13:20.617872 pinky.example.com > ijin.example.com: \
     AH(spi=0x0aaa749f,seq=0x335): ESP(spi=0x0ec0441e,seq=0x335) (DF)
```

6.5. Konfiguration von IPsec Netzwerk-zu-Netzwerk

Sie können IPsec auch so konfigurieren, dass ein ganzes Netzwerk (z.B. LAN oder WAN) mit einem Remote-Netzwerk mittels einer Netzwerk-zu-Netzwerk-Verbindung verbunden wird. Dafür müssen auf jeder Seite der zu verbindenden Netzwerke IPsec-Routers erstellt werden, damit Information verarbeitet werden und von einem Netzwerkknoten des Netzwerkes zu einem Knoten auf dem Remote-Netzwerk geroutet werden kann. Abbildung 6-1 zeigt eine Netzwerk-zu-Netzwerk-Verbindung mittels IPsec-Tunnel.

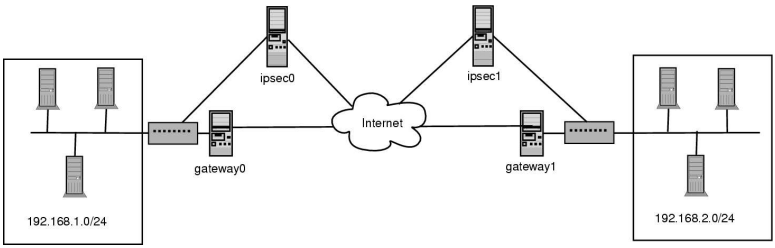

Abbildung 6-1. Eine Netzwerk-zu-Netzwerk-Verbindung mittels IPsec-Tunnel

Das Diagramm zeigt zwei separate LANs, die durch das Internet getrennt sind. Diese Netzwerke verwenden IPsec-Routers, um eine Verbindung in einem sicheren Tunnel im Internet zu authentifizieren und zu initialisieren. Pakete, die im Transit gefasst werden, müssten brute-force entschlüsselt werden, damit der Code geknackt werden kann, der die Pakete zwischen diesen LANs beschützt. Der

Prozess der Kommunikation von einem Netzknoten in der 192.168.1.0/24 IP-Reihe zu einem anderen auf 192.169.2.0/24 ist für die Knoten vollständig transparent, da die Verarbeiteng, die Ver- und Entschlüsselung und das Routing der IPsec-Pakete komplett vom IPsec-Router gehandhabt wird.

Die Information, die für eine Netzwerk-zu-Netzwerk-Verbindung gebraucht wird, umfasst:

- Die IP-Adressen der festgesetzten IPsec-Routers, auf die extern zugegriffen werden kann
- Die Netzwerk-Adressen-Reihen des LAN/WAN, die von den IPsec-Routers bedient werden (z.B. 192.168.0.0/24 or 10.0.1.0/24)
- Die IP-Adressen der Gateway-Einrichtungen, die die Daten von den Netzwerkknoten zum Internet leiten
- Einen einmaligen Namen, um die IPsec-Verbindung zu identifizieren und sie von anderen Geräten oder Verbindungen zu unterscheiden (z.B. `ipsec0`).
- Einen fixen Schlüssel zur Verschlüsselung oder einen, der automatisch von `racoon` geschaffen wurde.
- Ein 'vorinstallierter' Schlüssel zu Authentifikation, der verwendet wird, um die Verbindung zu initialisieren und den Austausch von Schlüsseln zur Verschlüsselung möglich zu machen.

Nehmen Sie z.B. an, LAN A (lana.example.com) und LAN B (lanb.example.com) wollen sich miteinender durch einen IPsec-Tunnel verbinden. Die Netzwerk-Adresse für LAN A liegt in der 192.168.1.0/24-Reihe, während LAN B die 192.168.2.254-Reihe verwendet. Die Gateway-IP Adresse ist 192.168.1.254 für LAN A und 192.168.2.254 für LAN B. Die IPsec-Router sind von jedem LAN-Gateway getrennt und verwenden zwei Netzwerk-Geräte: eth0 wird eine extern zugängliche statische IP-Adresse für das Internet zugeteilt, eth1 fungiert als Routing-Punkt für das Bearbeiten und Übertragen von LAN-Paketen von einem Netzwerkknoten zu den Remote-Netzwerkknoten.

Die IPsec-Verbindung zwischen den Netzwerken verwendet einen 'vorinstallierten' Schlüssel mit dem Wert `r3dh4tl1nux`. Die Administratoren von A und B einigen sich, `racoon` automatisch einen Authentifikations-Schlüssel zwischen den beiden IPsec-Routern erstellen zu lassen. Der Administrator von LAN A entscheidet sich dafür, die IPsec-Verbindung `ipsec0` zu nennen, während der Administrator von LAN B die IPsec-Verbindung `ipsec1` nennt.

Im folgenden sehen Sie die `ifcfg` Datei für eine Netzwerk-zu-Netzwerk-Verbindung mit IPsec für LAN A. Der einmalige Name zur Identifizierung der Verbindung ist in diesem Beispiel *`ipsec1`*, die daraus resultierende Datei heißt daher `/etc/sysconfig/network-scripts/ifcfg-ipsec1`.

```
TYPE=IPSEC
ONBOOT=yes
IKE_METHOD=PSK
SRCGW=192.168.1.254
DSTGW=192.168.2.254
SRCNET=192.168.1.0/24
DSTNET=192.168.2.0/24
DST=X.X.X.X
```

Die Verbindung ist so eingestellt, dass sie beim Hochfahren (`ONBOOT=yes`) startet. Sie verwendet die Authentifikations-Methode der vorher gemeinsam verwendeten Schlüsseln (`IKE_METHOD=PSK`). Der Administrator für LAN A gibt sowohl den Ziel-Gateway ein, der der Gateway für LAN B ist(`DSTGW=192.168.2.254`), als auch den Quell- Gateway, der die Gateway-IP-Adresse von LAN A ist(`SRCGW=192.168.1.254`). Der Administrator gibt dann sowohl das Ziel-Netzwerk ein, dass die Netzwerk-Reihe für LAN B ist(`DSTNET=192.168.2.0/24`) als auch das Quell- Netzwerk (`SRCNET=192.168.1.0/24`). Abschließend gibt der Administrator die Ziel-IP-Adresse ein, die die extern zugängliche IP-Adresse für LAN B ist (*`X.X.X.X`*).

Im folgenden finden Sie die Datei mit den 'vorinstallierten' Schlüsseln (`/etc/sysconfig/network-scripts/keys-ipsec`*`X`* genannt, wobei *`X`* die 0 für LAN A und

die 1 für LAN B ist), die beide Netzwerke verwenden, um sich gegenseitig zu authentifizieren. Der Inhalt dieser Datei sollte identisch sein und nur der root-Benutzer sollte die Datei lesen oder überschreiben können.

```
IKE_PSK=r3dh4tl1nux
```

Wichtig

Um die Datei `keys-ipsec` zu verändern, damit sie nur vom root-Benutzer gelesen oder bearbeitet werden kann, führen Sie nach der Erstellung der Datei den folgenden Befehl aus:

```
chmod 600 /etc/sysconfig/network-scripts/keys-ipsec1
```

Um den Authentifizierungs-Schlüssel jederzeit zu verändern, bearbeiten Sie die Datei `keys-ipsec`*X* bei beiden IPsec-Routern. *Für eine ordentliche Verbindung müssen beide Schlüssel gleich sein.*

Das ist die `/etc/racoon/racoon.conf`-Konfigurationsdatei für die IPsec-Verbindung. Beachten Sie, dass die `include`-Zeile am unteren Ende der Datei automatisch erstellt wird und nur dann erscheint, wenn gerade eine Verbindung mit einem IPsec-Tunnel vorhanden ist.

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

sainfo anonymous
{
 pfs_group 2;
 lifetime time 1 hour ;
 encryption_algorithm 3des, blowfish 448, rijndael ;
 authentication_algorithm hmac_sha1, hmac_md5 ;
 compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf"
```

Im folgenden sehen Sie die Konfigurationsdatei für die Verbindung zum Remote-Netzwerk. Die Datei trägt den Namen *X.X.X.X*`.conf` (ersetzen Sie *X.X.X.X* mit der IP Adresse des Remote-IPsec-Routers). Beachten Sie, dass diese Datei automatisch erzeugt wird, wenn der IPsec-Tunnel aktiviert wird. Sie sollte nicht direkt bearbeitet werden.

```
;
remote X.X.X.X
{
        exchange_mode aggressive, main;
        my_identifier address;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2 ;
        }
}
```

Bevor die IPsec-Verbindung gestartet wird, sollte IP-Forwarding beim Kernel eingestellt werden. Aktivieren Sie IP-Forwarding als root bei einem Shell Prompt:

1. Bearbeiten Sie `/etc/sysctl.conf` und stellen Sie `net.ipv4.ip_forward` to **`1`** ein.
2. Führen Sie den folgenden Befehl aus, damit die Änderung wirksam wird:
   `sysctl -p /etc/sysctl.conf`

Starten Sie die IPsec-Verbindung, indem Sie entweder die IPsec-Router neu starten oder den folgenden Befehl als root bei jedem Router eingeben:

```
/sbin/ifup ipsec0
```

Die Verbindungen sind nun aktiviert und LAN A und LAN B sind in der Lage, miteinander zu kommunizieren. Die Routen werden automatisch durch das Aufrufen des Initialisierungs-Skriptes mit `ifup` bei der IPsec-Verbindung erzeugt. Um eine Liste der Routen für das Netzwerk anzuzeigen, führen Sie folgenden Befehl aus:

```
/sbin/ip route list
```

Um die IPsec-Verbindung zu testen, führen Sie die `tcpdump` Utility auf dem extern routbaren Gerät aus (eth0 in diesem Beispiel). So können Sie die Netzwerk-Pakete sehen, die zwischen den Hosts (oder Netzwerken) übertragen werden, und überprüfen, dass sie über IPsec verschlüsselt werden. Um die IPsec-Verbindungsqualität z.B. für LAN A zu prüfen, geben sie folgendes ein:

```
tcpdump -n -i eth0 host lana.example.com
```

Das Paket sollte eine AH-Kopfzeile enthalten und sollte als ESP-Paket angezeigt werden. ESP heißt, dass es verschlüsselt ist. Zum Beispiel (ein inverser Schrägstrich kennzeichnet die Fortsetzung einer Zeile):

```
12:24:26.155529 lanb.example.com > lana.example.com: AH(spi=0x021c9834,seq=0x358): \
   lanb.example.com > lana.example.com: ESP(spi=0x00c887ad,seq=0x358) (DF) \
   (ipip-proto-4)
```

Kapitel 7.

Firewalls

Die Sicherheit von Informationen wird üblicherweise als Prozess und nicht als Produkt angesehen. Allerdings werden bei der Realisierung von standardmäßigen Sicherheitsvorgängen normalerweise gewisse Formen angepasster Mechanismen verwendet. So können Privilegien zugänglich gemacht und Netzwerke auf Benutzer beschränkt werden, die autorisiert, identifizierbar und rückverfolgbar sind. Red Hat Enterprise Linux enthält mehrere kompetente Tools, die Systemadministratoren und Sicherheitstechnikern bei Fragen der Netzwerklevel-Zugangskontrolle unterstützen können.

Zusammen mit VPN-Lösungen wie IPsec (siehe Kapitel 6) sind Firewalls einer der Kernbestandteile bei der Realisierung von Netzwersicherheit. Einige Vertreiber bieten Firewall-Lösungen an, die für alle Bereiche des Marktes geeignet sind: vom Heimbenützer, wo ein PC geschützt wird, bis hin zu Lösungen für Datenzentren, wo wichtige Unternehmensinformationen geschützt werden. Firewalls können alleinstehende Hardware-Lösungen sein, wie die Firewall-Einrichtungen von Cisco, Nokia und Sonicwall. Es gibt aber auch geschützte Software-Firewall-Lösungen für den Heim-und Firmenbereich, von Vertreibern wie z.B. Checkpoint, McAfee und Symantec.

Neben den Unterschieden zwischen Hardware- und Software-Firewalls gibt es auch Unterschiede in der Funktionsweise von Firewalls, die die verschiedenen Lösungen voneinander abheben. Tabelle 7-1 erklärt drei gängige Firewall-Typen und wie sie funktionieren:

Methode	Beschreibung	Vorteile	Nachteile
NAT	*Network Address Translation* (NAT) reiht Subnetzwerke von internen IP-Netzwerken hinter eine externe IP-Adresse oder eine kleine Gruppe von externen IP-Adressen. Alle Anfragen werden nur für eine Quelle maskiert, nicht für alle.	· Kann für Machinen an einem LAN · übersichtlich konfiguriert werden · Schützt viele Maschinen und Service hinter einer oder mehreren IP-Adresse(n). Vereinfacht die Aufgaben der Systemadministratoren · Durch das Öffnen und Schließen von Ports an der NAT Firewall/Gateway kann eine Benutzerbeschränkung zu und von dem LAN konfiguriert werden	· Kann keine bösartigen Aktivitäten verhindern, sobald der Benutzer mit einem Service außerhalb der Firewall verbunden ist

Methode	Beschreibung	Vorteile	Nachteile
Paketfilter	Paketfilter-Firewalls lesen alle Datenpakete, die sich innerhalb und außerhalb eines LAN bewegen. Pakete können mit Hilfe der Kopfzeileninformation gelesen und bearbeitet werden. Die Pakete werden auf der Grundlage von programmierbaren Regeln gefiltert werden, die vom Systemadministrator der Firewall aufgestellt wurden. Der Linux Kernel hat eine eingebaute Paketfilterfunktion über das Netfilter Kernel Subsystem.	· Anpassbar durch das `iptables` front-end utility · Erfordert keine Anpassung auf Seiten des Client, da alle Netzwerkaktivitäten auf Router-Level und nicht auf Ebene der Anwendung gefiltert werden · Da Pakete nicht durch ein Proxy übertragenwerden, ist das Netzwerk aufgrund direkter Verbindung vom Client zum Remote Host schneller	· Kann Pakete nicht nach Inhalt filtern wie Proxy Firewalls · Verarbeitet Pakete auf dem Protokoll Layer, aber kann sie nicht auf dem Layer der Anwendungen filtern · Eine komplizierte Netzwerkarchitektur kann das Erstellen von Regeln zur Paketfilterung schwierig machen, im Speziellen, wenn sie mit *IP masquerading* oder mit lokalen Subnetzen und DMZ-Netzwerken gekoppelt sind
Proxy	Proxy-Firewalls filtern alle Anfragen eines bestimmten Protokolls oder Typs von den LAN-Clients zu einer Proxy-Maschine, von wo aus die Anfragen im Namen des lokalen Clients an das Internet gestellt werden. Eine Proxy Maschine fungiert als ein Buffer zwischen bösartigen Benutzern von außen und den internen Client-Maschinen des Netzwerkes.	· Gibt dem Administrator Kontrolle darüber, welche Anwendungen und Protokolle außerhalb des LAN funktionieren · Manche Proxy-Server können Daten, auf welche häufig zugegriffen wird, in einer Cache-Datei speichern, damit Clients Zugang zu oftmals gebrauchten Daten von der lokalen Cache-Datei haben, anstelle die Internetverbindung benützen zu müssen. Dies ist hilfreich beim Einsparen von unnötigem Bandbreitenkonsum. · Proxy-Dienste können genau dokumentiert und beobachtet werden, was bessere Kontrolle bezüglich der Nutzung von Netzwerkressourcen ermöglicht	· Proxies sind oft anwendungsspezifisch (HTTP, telnet, etc.) oder protokollbeschränkt (die meisten Proxies arbeiten nur mit TCP-verbundenen Servicen) · Die Dienste von Anwendungen können nicht hinter einem Proxy laufen, daher müssen Ihre Anwendungsserver eine andere Form von Netzwerksicherheit verwenden Proxies können zu einer Engstelle in einem Netzwerk werden, da alle Anfragen und Übetragungen durch eine Quelle gehen im Gegensatz zu direkten Verbindungen vom Client zum Remote Service

Tabelle 7-1. Firewall-Typen

7.1. Netzfiler und `iptables`

Der Linux Kernel enthält ein kompetentes Netzwerk-Subsystem mit dem Namen *Netfilter*. Das Netfilter-Subsystem bietet eine Paketfilterung mit oder ohne Status sowie NAT- und IP-Maskierungsdienste. Netfilter hat auch die Möglichkeit, IP-Kopfzeileninformation für

fortgeschrittenes Routing und zur Überprüfung des Verbindungszustandes zu überarbeiten (*mangle*). Netfilter wird durch das `iptables`-Utility kontrolliert.

7.1.1. `iptables`-Überblick

Die Kompetenz und Flexibilität von Netfilter wird durch die `iptables`-Schnittstelle erreicht. Dieses Tool für die Befehlszeile ist syntaxgleich zu seinem Vorläufer `ipchains`. `iptables` verwendet jedoch das Netfilter-Subsystem, um die Netzwerkverbindung, die Inspektion und die Verarbeitung zu verbessern, während `ipchains` komplizierte Regeln zur Filterung von Quell- und Zielpfaden sowie zugehörige Verbindungsports verwendete. `iptables` bietet in einer Befehlszeilen-Schnittstelle fortschrittliche Dokumentation, Vor- und Nachrouting-Aktionen, Übersetzung von Netzwerkadressen und Port-Weiterleitung

Dieser Abschnitt enthält eine Übersicht über `iptables`. Für genauere Informationen über `iptables` siehe das *Red Hat Enterprise Linux Referenzhandbuch*.

7.2. Verwendung von `iptables`

Der erste Schritt bei der Verwendung von `iptables` ist, den `iptables`-Dienst zu starten. Führen Sie folgenden Befehl aus:

```
service iptables start
```

Warnung

Die `ip6tables`-Dienste sollten abgeschaltet sein, wenn IPTables mit dem folgenden Befehl verwendet wird:

```
service ip6tables stop
chkconfig ip6tables off
```

Damit `iptables` immer standardmäßig startet, wenn das System hochgefahren wird, müssen Sie mit `chkconfig` den Runlevel-Status ändern.

```
chkconfig --level 345 iptables on
```

Die Syntax von `iptables` ist in Stufen unterteilt. Die Hauptstufe ist die *Kette*. Eine Kette (Chain) setzt den Satus fest, bei dem ein Paket manipuliert wird. Die Verwendung sieht so aus:

```
iptables -A chain -j target
```

`-A` fügt eine Regel an das Ende eines existierenden Regelsystems an. *`Kette`* ist der Name der Kette für eine Regel. Die drei eingebauten Ketten von `iptables` sind INPUT, OUTPUT und FORWARD. (Dies sind die Ketten, die auf jedes Paket einwirken, das ein Netzwerk durchläuft.) Diese Ketten sind permanent und können nicht gelöscht werden. Die `-j` *`target`*-Option legt den Ort im `iptables`-Regelsystem, wohin diese bestimmte Regel *springen* sollte.

Neue Ketten (auch benutzerdefinierte Ketten genannt) können mittels der `-N`-Option erstellt werden. Eine neue Kette zu erzeugen ist nützlich zum Anpassen von granularen oder aufwendigen Regeln.

7.2.1. Grundlegende Firewall-Richtlinien

Die Festlegung grundlegender Firewall-Richtlinien ist das Fundament auf dem mehr benutzerdefinierte und detaillierte Regeln erstellt werden können. `iptables` verwendet Richtlinien (`-P`), um standardmäßige Regeln zu erstellen. Sicherheitsbewusste Administratoren entscheiden sich normalerweise für die Norm, alle Pakete auszulassen und nur bestimmte Pakete auf einer Fall-zu-Fall-Basis zu genehmigen. Die folgenden Regeln blockieren alle eingehenden und ausgehenden Pakete am Gateway eines Netzwerkes:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Zusätzlich wird empfohlen, dass jeder *forwarded packets* — Netzwerkverkehr, der von der Firewall zu seinem Zielknoten geleitet werden soll, ebenfalls verhindert wird. Interne Clients werden so vor unabsichtlichem Kontakt mit dem Internet geschützt. Benützen Sie hierfür folgende Regel:

```
iptables -P FORWARD DROP
```

Nachdem die Ketten gemäß der Richtlinien eingestellt sind, können Sie neue Regeln für Ihre besonderen Netzwerk- und Sicherheitsbedürfnisse erstellen. Im Folgenden sind einige Regeln beschrieben, die sie beim Aufbau Ihrer `iptables`-Firewall verwenden können.

7.2.2. Speichern und Wiederherstellen von `iptables`-Regeln

Firewall-Regeln sind nur aktiv, wenn der Computer läuft. Wenn Sie das System neu starten, werden die Regeln automatisch gelöscht und rückgestellt. Verwenden Sie folgenden Befehl, um die Regeln zu speichern, damit sie nachher wieder geladen werden können:

```
/sbin/service iptables save
```

Die Regeln werden in der Datei `/etc/sysconfig/iptables`gespeichert und werden immer dann aktiviert, wenn das Service gestartet oder neu gestartet wird, auch wenn das System neu hochgefahren wird.

7.3. Übliche `iptables` Filterung

Fremde Angriffe von einem LAN fernzuhalten, ist ein wichtiger Aspekt der Netzwerksicherheit, wenn nicht *der Wichtigste*. Die Integrität eines LAN sollte durch die Verwendung strenger Firewall-Regeln vor bösartigen auswärtigen Benutzern geschützt werden. Mit Standard-Richtlinien, die alle eingehenden, ausgehenden und weitergeleiteten Pakete blockieren, ist es allerdings Firewall/Gateway- und internen LAN-Benutzern nicht möglich, miteinander oder extern zu kommunizieren. Damit die Benutzer Netzwerk-bezogene Funktionen ausüben und Netzwerk-Anwendungen verwenden können, müssen die Administratoren bestimmte Ports für die Kommunikation öffnen.

Um Beispielsweise Zugang zu Part 80 *an der Firewall* zu ermöglichen, fügen Sie die fogende Regel hinzu:

```
iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

Dies ermöglicht normales Webbrowsing von Websites, die über Port 80 kommunizieren. Um Zugang zu sicheren Websites zu erhalten (wie z.B. https://www.example.com/), müssen Sie auch Port 443 öffnen:

```
iptables -A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Wichtig

Wenn ein `iptables`-Regelsystem erstellt wird, darf nicht vergessen werden, dass die Reihenfolge wichtig ist. Wenn z.B. eine Kette festlegt, dass alle Pakete des lokalen 192.168.100.0/24 Subnetzes ausgelassen werden und dann eine Kette angefügt wird (`-A`), die Pakete von 192.168.100.13 (dies liegt innerhalb des ausgelassenen beschränkten Subnetzes) genehmigt, dann wird die angefügte Regel ignoriert. Sie müssen in diesem Fall zuerst eine Regel aufstellen, die 192.168.100.13 genehmigt, und dann eine Auslassungsregel im Subnetz erstellen.

Um willkürlich eine Regel in eine existierende Kette von Regeln einzufügen, verwenden Sie `-I` gefolgt von der Kette, in der Sie die Regel einfügen wollen und einer Regelnummer (1,2,3,...,n) die besagt, wo die Regel liegt. Zum Beispiel:

```
iptables -I INPUT 1 -i lo -p all -j ACCEPT
```

Die Regel wird als erste Regel in der INPUT-Kette eingefügt, damit Verkehr von einer lokalen Loopback-Einrichtung möglich wird.

Es mag Zeiten geben, in denen Sie einen Zugang zum LAN von außerhalb des LAN herstellen wollen. Für einen verschlüsselten Zugang von außen können Sie sichere Services wie SSH oder CIPE verwenden. Administratoren mit PPP-Ressourcen (wie Modem-Banken oder ISP-Massenkonten) können Einwahl-Verbindungen verwenden, um Firewall-Barrieren sicher zu umgehen. Modemverbindungen sind direkte Verbindungen und befinden sich typischerweise hinter Firewalls/Gateways. Für Fernbenutzer mit Breitband-Verbindungen können spezielle Einstellungen gemacht werden. Sie können `iptables` so konfigurieren, dass Verbindungen von entfernt liegenden SSH-Clients akzeptiert werden. Verwenden Sie die folgenden Regeln, um zum Beispiel einen SSH-Zugang von außen zu ermöglichen:

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
```

Es gibt noch andere Dienste, für die Sie Regeln definieren müssen. Siehe *Red Hat Enterprise Linux Referenzhandbuch* für ausführliche Informationen über die zahlreichen Optionen von `iptables` und über `iptables` selbst.

Diese Regeln erlauben eingehenden und ausgehenden Zugang für ein individuelles System, wie einen Einzel-PC, der direkt mit dem Internet oder Firewall/Gateway verbunden ist. Sie erlauben jedoch keinen Zugang zu diesen Diensten für Netzwerkknoten hinter der Firewall. Sie können NAT mit `iptables`-Filterregeln verwenden, um LAN-Zugang zu diesen Diensten zu ermöglichen.

7.4. FORWARD und NAT Regeln

Den meisten Organisationen wird eine limitierte Anzahl von öffentlich routbaren IP-Adressen von ihrem ISP zugewiesen. Aufgrund dieser Einschränkungen müssen die Administratoren kreative Wege finden, den Zugang zum Internet aufzuteilen, ohne dass jedem Knoten am LAN kostbare IP-Adressen zugeteilt werden. Der normale Weg, damit alle Knoten auf einem LAN die Netzwerkdienste intern und extern nützen können, ist die Verwendung von privaten IP-Adressen. Edge Routers (wie Firewalls) können eingehende Übertragungen vom Internet empfangen und die Pakete zu den gewünschten LAN-Knoten leiten. Gleichzeitig können Firewalls/Gateways auch ausgehende Anfragen von einem LAN-Knoten zu dem entfernten Internetdienst leiten. Dieses Weiterleiten des Netzwerkverkehrs kann manchmal gefährlich werden, vor allem, wenn moderne Cracking Tools verwendet werden, die *interne* IP-Adressen austricksen können und den Computer des externen Angreifers wie einen Netzwerkknoten des LAN erscheinen lassen. Zur Vorbeugung bietet `iptables` Richtlinien zum

Routing und Weiterleiten, die eingesetzt werden können, um fälschlicher Verwendung von Netzwerk-Ressourcen vorzubeugen.

Die `FORWARD` Richtlinie erlaubt einem Administrator zu kontrollieren, wohin die Pakete innerhalb eines LAN geroutet werden können. Wenn z.B. ein Weiterleiten an den gesamten LAN erlaubt werden soll (angenommen, die Firewall/Gateway hat eine interne IP-Adresse auf eth1), können die folgenden Regeln eingestellt werden.

```
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -o eth1 -j ACCEPT
```

Diese Regel ermöglicht Systemen hinter der Firewall/dem Gateway Zugang zum internen Netzwerk. Der Gateway leitet Pakete von einem LAN-Knoten zu dessem beabsichtigten Ziel-Knoten, indem alle Pakete durch dessen `eth1`-Gerät durchlaufen.

Anmerkung

Die IPv4 Richtlinie in Red Hat Enterprise Linux Kernels verhindert standardmäßig die Unterstützung von IP-Weiterleitung, was verhindert, dass Boxen, die Red Hat Enterprise Linux ausführen, als zugeordnete Edge Router fungieren. Führen Sie den folgenden Befehl aus, um IP-Weiterleitung einzuschalten:

```
sysctl -w net.ipv4.ip_forward=1
```

Wenn dieser Befehl über einen Shell-Prompt ausgeführt wird, wird die Einstellung nach einem Neustart nicht behalten. Sie können permanentes Weiterleiten einstellen, indem Sie die `/etc/sysctl.conf` Datei bearbeiten. Suchen Sie die folgende Zeile und ersetzen Sie `0` mit `1`:

```
net.ipv4.ip_forward = 0
```

Führen Sie den folgenden Befehl aus, um die Änderung der `sysctl.conf` Datei zu ermöglichen:

```
sysctl -p /etc/sysctl.conf
```

Dies erlaubt LAN-Netzwerkknoten, miteinander zu kommunizieren. Es ist ihnen jedoch nicht gestattet, extern (zum Beispiel mit dem Internet) zu kommunizieren. Um LAN-Netzwerkknoten mit privaten IP-Adressen das Kommunizieren mit externen öffentlichen Netzwerken zu ermöglichen, konfigurieren Sie die Firewall für *IP-Masquerading*. Dies maskiert Anfragen der LAN-Netzwerkknoten mit der IP-Adresse der äußeren Einstellung der Firewall (in diesem Fall eth0):

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Die Regel benutzt die NAT-Paketverwaltungstabelle (Packet Matching) (`-t nat`) und legt die eingebaute POSTROUTING-Kette für NAT(`-A POSTROUTING`) auf dem externen Netzwerkgerät der Firewall fest (`-o eth0`). POSTROUTING erlaubt es Paketen abgeändert zu werden, da diese das externe Gerät der Firewall verlassen. Das `-j MASQUERADE`-Target-Option ist festgelegt, um die private IP-Adresse eines Knotens mit der externen IP-Adresse der Firewall/des Gateways zu maskieren.

Wenn Sie einen Server in Ihrem internen Netzwerk extern zugänglich machen möchten, können Sie die Target-Option `-j DNAT` der PREROUTING-Kette in NAT dazu verwenden, Ziel-IP-Adresse und Port festzulegen, wo eingehende Pakete, die um eine Verbindung mit Ihrem internen Service anfragen, weitergeleitet werden können. Wenn Sie zum Beispiel eingehende HTTP-Anfragen an Ihr Apache HTTP Server Server-System auf IP-Adresse 172.31.0.23 weiterleiten möchten, führen Sie folgenden Befehl aus:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
```

```
--to 172.31.0.23:80
```

Diese Regel legt fest, dass die NAT-Tabelle die eingebaute PREROUTING-Kette zur Weiterleitung eingehender HTTP-Anfragen ausschließlich an die gelistete Ziel-IP-Adresse von 172.31.0.23 benutzt.

Anmerkung

Wenn sich die Standardmethode DROP in Ihrer FORWARD-Kette befindet, müssen Sie eine Regel anhängen, die das Weiterleiten von eingehenden HTTP-Anfragen ermöglicht, sodass das Ziel-NAT-Routing ermöglicht wird. Führen Sie dazu folgenden Befehl aus:

```
iptables -A FORWARD -i eth0 -p tcp --dport 80 -d 172.31.0.23 -j ACCEPT
```

Die Regel erlaubt das Weiterleiten von eingehenden HTTP-Anfragen von der Firewall zu deren vorgesehenem Ziel auf dem Apache HTTP Server-Server hinter der Firewall.

7.4.1. DMZs und `iptables`

`iptables`-Regeln können dafür verwendet werden, den Verkehr zu bestimmten Maschinen zu leiten, wie zum Beispiel einem zweckbestimmten HTTP- oder FTP-Server in einer *demilitarisierten Zone* (DMZ) — ein spezielles lokales Subnetzwerk, das dazu bestimmt ist Dienste öffentlich, z.B. im Internet, anzubieten. Um eine Regel für das Routen von allen eingehenden HTTP-Anfragen zu einem ausgewiesenen HTTP-Server auf IP-Adresse 10.0.4.2 festzulegen (außerhalb der 192.168.1.0/24 Reichweite des LAN), ruft Network Address Translation (NAT) eine `PREROUTING`-Tabelle auf. Damit werden die Pakete an das richtige Ziel weitergeleitet:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
     --to-destination 10.0.4.2:80
```

Mit diesem Befehl werden alle HTTP-Verbindungen zu Port 80 von außerhalb des LAN auf den HTTP-Server in ein vom Rest des internen Netzwerks getrenntes Netzwerk geleitet. Diese Art der Netzwerksegmentierung kann sicherer sein, als wenn die HTTP-Verbindungen auf einer Maschine im Netzwerk gestattet werden. Wenn der HTTP-Server so konfiguriert ist, dass er sichere Verbindungen akzeptiert, dann muss auch Port 443 weitergeleitet werden.

7.5. Viren und geknackte IP-Adressen

Es können auch kompliziertere Regeln erstellt werden, die den Zugang zu bestimmten Subnetzwerken oder sogar Netzwerkknoten innerhalb eines LAN kontrollieren. Man kann auch diverse dubiose Dienste einschränken, wie Trojans, Worms und andere Client/Server Viren. Es gibt zum Beispiel einige Trojans, die Netzwerke nach Diensten durchsuchen, und zwar von Port 31337 bis 31340 (in der Cracker-Sprache die *elitären*Ports genannt). Da es keine legitimierten Dienste gibt, die mit diesen nicht standardmäßigen Ports kommunizieren, kann das Blockieren dieser Ports die Chance, dass potentiell infizierte Netzwerkknoten in Ihrem Netzwerkes unabhängig mit ihren auswärtigen Master-Servern kommunizieren, so gering als möglich gehalten werden.

```
iptables -A OUTPUT -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
iptables -A FORWARD -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
```

Sie können auch Verbindungen von außen blockieren, die versuchen, eine Reihe von privaten IP-Adressen zu knacken, um Ihren LAN infiltrieren zu können. Wenn Ihr LAN die 192.168.1.0/24 Reihe verwendet, kann zum Beispiel eine Regel aufgestellt werden, dass alle Pakete ausgelassen werden, die

eine IP-Adresse haben, wie sie in Ihrem LAN vorkommt. Da als Standard-Richtlinie empfohlen wird, weitergeleitete Pakete zurückzuweisen, werden auch andere geknackte IP-Adressen automatisch vom nach außen gerichteten Gerät (eth0) zurückgewiesen.

```
iptables -A FORWARD -s 192.168.1.0/24 -i eth0 -j DROP
```

Anmerkung

Beim Arbeiten mit *appended*-Regeln wird zwischen den `REJECT`- und `DROP`-Zielaktionen unterschieden. `REJECT` verweigert den Zugriff und zeigt bei Benutzern, die versuchen, sich mit dem Service zu verbinden, einen `connection refused` Error an. `DROP` lässt das Paket ohne jede Warnung für `telnet` Benutzer aus. Die Administratoren können diese Aktionen nach ihrem eigenem Ermessen verwenden. Es wird allerdings `REJECT` empfohlen, um Verwirrung beim Benutzer und wiederholte Verbindungsversuche zu vermeiden.

7.6. `iptables` und dynamische Paketfilterung

`iptables` beinhaltet ein Modul, welches Administratoren erlaubt, Verbindungen zu Diensten auf einem internen Netzwerk zu überprüfen und einzuschränken mittels einer Methode, die *Connection Tracking* oder auch *Dynamische Paketfilterung* genannt wird. Dynamische Paketfilterung legt eine Tabelle an, welche es Administratoren ermöglicht, Zugang zu erlauben oder abzulehnen, basierend auf folgenden Verbindungs-Zuständen:

- `NEW` — Ein Paket fragt eine neue Verbindung an, wie z.B. eine HTTP-Anfrage.
- `ESTABLISHED` — Ein Paket, welches Teil einer bestehenden Verbindung ist.
- `RELATED` — Ein Paket, welches eine neue Verbindung anfragt, jedoch Teil einer bestehenden Verbindung ist, wie z.B. passive FTP-Verbindungen, wo der Verbindungsport 20 ist und der Transfer- oder Übertragungs-Port jeder unbenutzte Port 1024 und höher sein kann.
- `INVALID` — Ein Paket, welches kein Teil irgendeiner Verbindung in der dynamischen Paketfilterungstabelle ist.

Sie können die Zustandsfunktionalität der dynamischen Paketfilterung von `iptables` mit jedem Netzwerkprotokoll benutzen, auch wenn das Protokoll selbst statuslos ist (wie z.B. UDP). Das folgende Beispiel zeigt eine Regel, welche dynamische Paketfilterung dazu benutzt, um nur die Pakete, die mit einer unzweifelhaften Verbindung in Zusammenhang stehen.

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ALLOW
```

7.7. `ip6tables`

Die Einführung des Internet-Protokolls der nächsten Generation, IPv6 genannt, erweitert die Möglichkeiten des 32-Bit-Adressenlimits von IPv4 (oder IP). IPv6 unterstützt 128-Bit-Adressen und daher können IPv6 kompatible Träger-Netzwerke eine größere Anzahl routbarer Adressen ansprechen als mit IPv4.

Red Hat Enterprise Linux unterstützt die IPv6 Firewall-Regeln unter Verwendung des Netfilter 6 Subsystems und des `ip6tables`-Befehls. Der erste Schritt bei der Verwendung von `ip6tables` ist das Starten des `ip6tables`-Dienstes mit folgendem Befehl:

```
service ip6tables start
```

Warnung

Die `iptables`-Dienste müssen abgeschaltet sein, damit der `ip6tables`-Dienst exklusiv benutzt werden kann:

```
service iptables stop
chkconfig iptables off
```

Damit `ip6tables` standardmäßig startet, wann immer das System hochgefahren wird, müssen Sie den Runlevel Status mit `chkconfig` ändern.

```
chkconfig --level 345 ip6tables on
```

Die Syntax ist identisch mit `iptables`, außer dass `ip6tables` 128-Bit-Adressen unterstützt. SSH-Verbindungen auf einem IPv6-kompatiblen Netzwerk können z.B. mt der folgenden Regel aktiviert werden:

```
ip6tables -A INPUT -i eth0 -p tcp -s 3ffe:ffff:100::1/128 --dport 22 -j ACCEPT
```

Für mehr Information über IPv6 Networking siehe die IPv6 Informationsseiteunter http://www.ipv6.org/.

7.8. Zusätzliche Informationsquellen

Einige Aspekte von Firewalls und des Linux-Netfilter-Subsystems konnten in diesem Kapitel nicht abgedeckt werden. Für weitere Informationen ziehen Sie bitte die folgenden Quellen zu Rate:

7.8.1. Installierte Dokumentation

- Das *Red Hat Enterprise Linux Referenzhandbuch* beinhaltet ein ausführliches Kapitel über `iptables`, einschließlich der Definitionen für alle Befehlsoptionen.
- Die `iptables` man-Seite enthält ebenfalls eine kurze Zusammenfassung der verschiedenen Optionen.
- In Anhang C und in `/etc/services` befindet sich eine Liste der gebräuchlichen Dienste und ihrer Port Nummern.

7.8.2. Hilfreiche Websites

- http://www.netfilter.org/ — Die offizielle Homepage des Netfilter und `iptables` Projekts.
- http://www.tldp.org/ — Das Linux-Dokumentations-Projekt enthält mehrere hilfreiche Anweisungen in Zusammenhang mit der Erstellung und Administration von Firewalls.
- http://www.iana.org/assignments/port-numbers — Die offizielle Liste registrierter und üblicher Service-Ports, zugeteilt von der Internet Assigned Numbers Authority.

7.8.3. Verwandte Dokumentation

- *Red Hat Linux Firewalls*, von Bill McCarty; Red Hat Press — eine umfassende Referenz beim Erstellen von Netzwerk- und 'Open Source'-Firewalls mittels Open Source Paketfilterungs-Technologie wie z.B. Netfilter und `iptables`. Es beinhaltet Themen wie beispielsweise das Analysieren von Firewall-Logs, das Entwickeln von Firewall-Regeln und das Anpassen Ihrer Firewall mit grafischen Tools wie z.B. `lokkit`.
- *Linux Firewalls*, von Robert Ziegler; New Riders Press. — enthält eine Menge an Informationen über das Erstellen von Firewalls mit 2.2 kernel und `ipchains` sowie mit Netfilter und `iptables`. Es werden auch zusätzliche Sicherheitsthemen abgedeckt, wie Probleme mit Zugang von außen und Erkennungssysteme bei Eindringen.

III. Sicherheit einschätzen

Dieser Abschnitt bietet einen Überblick über Theorie und Praxis der Sicherheitseinschätzung. Von Tools zum Überwachen eines Netzwerks zu Cracking-Tools, ein Administrator kann mehr über das Sichern eines Systems und Netzwerks erfahren, wenn dieser selbst in diese einbricht.

Inhaltsverzeichnis

8. Schwachstellenanalyse 79

Kapitel 8.

Schwachstellenanalyse

Mit genügend Zeit, Ressourcen und Motivation kann ein Cracker in fast jedes System einbrechen. Schlussendlich stellen alle derzeit erhältlichen Technologien und Sicherheitsprozeduren keine Garantie dar, dass irgendein System vor Eindringlingen sicher ist. Router können bei der Sicherung Ihrer Gateways zum Internet helfen. Firewalls helfen bei der Sicherung des Netzwerks. Virtuelle Private Netzwerke können auf sichere Art Daten verschlüsselt übertragen. Intrusion-Detection-Systeme können Sie vor böswilligen Aktivitäten warnen. Der Erfolg jeder dieser Technologien hängt jedoch von einer Reihe von Variablen ab. Diese sind unter anderem:

- Die Kompetenz der Mitarbeiter, die für die Konfiguration, Überwachung und Wartung dieser Technologien verantwortlich sind.
- Die Fähigkeit, Services und Kernel schnell und effizient mit Patches versehen und aktualisieren zu können.
- Die Fähigkeit der Verantwortlichen, konstante Wachsamkeit im Netzwerk auszuüben.

Durch den dynamischen Zustand von Datensystemen und Technologien kann das Sichern Ihrer Ressourcen ziemlich komplex werden. Aufgrund dieser Komplexität kann es sich schwierig gestalten, Experten für Ihre Ressourcen zu finden. Es ist zwar möglich, Mitarbeiter mit reichhaltigem Wissen auf vielen Gebieten der Informationssicherheit zu beschäftigen, aber es ist relativ schwierig, Experten auf nur wenigen Gebieten zu behalten. Dies liegt hauptsächlich daran, dass die Informationssicherheit ständige Aufmerksamkeit und Fokus verlangt. Informationssicherheit ist ein ständig im Wandel begriffener Prozess.

8.1. Denken wie der Feind

Angenommen, Sie verwalten ein Firmennetzwerk. Solche Netzwerke bestehen meistens aus Betriebssystemen, Applikationen, Servern, Netzwerküberwachung, Firewalls, Intrusion-Detection-Systemen und vielem mehr. Stellen Sie sich jetzt vor, Sie müssen dahingehend immer auf dem neuesten Stand sein. Durch die Komplexität heutiger Software und Netzwerkumgebungen sind Angriffe auf einen Rechner unter Ausnutzung eines Sicherheitslochs und Bugs eine Gewissheit. Mit allen Patches und Updates für ein gesamtes Netzwerk auf dem Laufenden zu sein, ist eine gewaltige Aufgabe innerhalb eines großen Unternehmens mit heterogenen Systemen.

Wenn Sie nun diese gewaltigen Anforderungen an das Wissen mit der Aufgabe, immer auf dem neuesten Stand zu sein, kombinieren, sind Vorfälle, Systemeinbrüche, Datenkorruption und Serviceunterbrechungen unvermeidbar.

Um den Nutzen dieser Sicherheitstechnologien zu erhöhen und dabei zu helfen, Systeme, Netzwerke und Daten zu schützen, sollten Sie sich in die Lage eines Crackers versetzen und die Sicherheit der Systeme durch das Suchen von Schwachstellen testen. Vorbeugende Schwachstellenanalysen für Ihre eigenen Systeme und Netzwerkressourcen können potentielle Problemstellen aufdecken, bevor ein Cracker diese zu seinem Vorteil ausnutzen kann.

Eine Schwachstellenanalyse ist eine interne Prüfung Ihrer Netzwerk- und Systemsicherheit. Die Ergebnisse zeigen die Vertraulichkeit, Integrität und Verfügbarkeit Ihres Netzwerks auf (wie in Abschnitt 1.1.4 beschrieben). Eine Schwachstellenanalyse beginnt für gewöhnlich mit einer Erkundungsphase, in der wichtige Daten zum System und Ressourcen gesammelt werden. Diese Phase führt zur Systembereitschaftsphase, in der das Ziel auf alle bekannten Schwachstellen hin geprüft wird. Diese Phase führt dann zur Berichterstattungsphase, in der die Ergebnisse in die Risiko-Kategorien Hoch, Mittel und Niedrig eingestuft und Methoden zur Verbesserung der Sicherheit (oder Schwächung der Anfälligkeit) diskutiert werden.

Würden Sie zum Beispiel eine Schwachstellenanalyse für Ihr Haus durchführen, würden Sie wahrscheinlich prüfen, ob jede Tür geschlossen und auch abgeschlossen ist. Sie würden auch jedes Fenster prüfen und sicherstellen, dass diese richtig schließen und abgeschlossen werden können. Das gleiche Konzept gilt auch für Systeme, Netzwerke und elektronische Daten. Benutzer mit böswilligen Absichten sind die Diebe und Vandalen Ihrer Daten. Konzentrieren Sie sich auf deren Tools, Mentalität und Beweggründe, denn so können Sie schnell auf deren Taten reagieren.

8.2. Definition von Analyse und Test

Schwachstellenanalysen können in zwei Arten klassifiziert werden: *von außen innen herumschnüffeln* und *innen herumschnüffeln*.

Wenn Sie eine Schwachstellenanalyse von außen betrachtet durchführen, so versuchen Sie, Ihr System von außen zu beeinflussen. Wenn Sie Ihre Firma extern betrachten, gibt Ihnen dies die Sichtweise eines Crackers. Sie sehen, was der Cracker sehen kann — öffentlich-weiterleitbare IP-Adressen, Systeme auf Ihrer *DMZ*, externe Schnittstellen Ihrer Firewall und vieles mehr. DMZ steht für "Demilitarized Zone", was einem Computer oder einem kleinen Subnetzwerk entspricht und welche sich zwischen einem internen, zuverlässigen Netzwerk befindet, wie z.B. einem gemeinschaftlichen privaten LAN und einem unzuverlässigen, externen Netzwerk, wie z.B. das öffentliche Internet. Üblicherweise beinhaltet die DMZ Geräte, die für den Internetverkehr zugänglich sind, wie z.B. Web(HTTP)-Server, FTP-Server, SMTP(E-Mail)-Server und DNS-Server.

Wenn Sie eine Schwachstellenanalyse von innen betrachtet durchführen, haben Sie den gewissen Vorteil, das Sie bereits intern sind, und Sie einen Status des vertrauens haben. Dies ist der Blickwinkel, den Sie und Ihre Kollegen haben, wenn Sie sich einmal im System angemeldet haben. Sie sehen Druckserver, Dateiserver, Datenbanken und andere Ressourcen.

Es gibt klare Unterschiede zwischen diesen beiden Arten der Schwachstellenanalyse. Als interner Mitarbeiter Ihres Unternehmens besitzen Sie erhöhte Privilegien — weit mehr als jeder Außenstehende. In den meisten Unternehmen sind Sicherheitsvorkehrungen derartig getroffen, um Eindringlinge fernzuhalten. Es wird nur sehr wenig für die interne Sicherung des Unternehmens getan (z.B. Firewalls für Abteilungen, Zugangskontrollen auf Benutzerebene, Authentifizierungsvorgänge für interne Ressourcen und so weiter. Üblicherweise gibt es wesentlich mehr Ressourcen, wenn man sich intern umschaut, da die meisten Systeme in einem Unternehmen intern sind. Sobald Sie sich einaml außerhalb eines Unternehmens befinden, erhalten Sie sofort den Status vertrauensunwürdig zu sein. Die extern zugänglichen Systeme und Ressourcen sind für gewöhnlich wesentlich stärker eingeschränkt.

Betrachten Sie die Unterschiede zwischen Schwachstellenanalyse und *Eindringungstests*. Sehen Sie die Schwachstellenanalyse als ersten Schritt zu einem Eindringungstest an. Die Informationen aus der Schwachstellenanalyse werden im Test angewendet. Mit der Analyse wird nach Löchern und möglichen Schwachstellen im System gesucht, während der Eindringungstest die Ergebnisse in die Tat umsetzt.

Die Einschätzung der Netzwerk-Infrastruktur ist ein dynamischer Prozess. Das Durchführen der Analyse gibt einen Überblick über positive sowie negative Aspekte.

Sicherheits-Administratoren sind nur so gut wie die Tools, die diese benutzen, und das Wissen, das diese bewahren. Nehmen Sie eines der aktuell erhältlichen Analysetools und lassen Sie es über Ihr System laufen Dabei ist fast garantiert, dass einige Schwachstellen gefunden werden, die gar nicht existieren. Ob durch einen Programmfehler oder Benutzerfehler hervorgerugen, das Ergebnis ist das gleiche. Das Tool findet Schwachstellen, die gar nicht existieren, oder schlimmer noch, findet wirklich existierende Schwachstellen nicht.

Da wir nun den Unterschied zwischen Schwachstellenanalyse und Eindringungstest definiert haben, ist es ratsam, die Ergebnisse der Analyse sorgfältig zu prüfen, bevor Sie den Eindringungstest tatsächlich durchführen.

Achtung

Der Versuch, Schwachstellen in Produktionsressourcen aufzudecken, kann einen negativen Effekt auf die Produktivität und Effizienz Ihrer Systeme und Netzwerke haben.

In der folgenden Liste werden einige der Vorteile einer Schwachstellenanalyse aufgezeigt.

- Proaktiver Fokus auf Informationssicherheit
- Auffinden potentieller Schwachstellen, bevor diese von Crackern gefunden werden
- Resultiert normalerweise darin, dass Systeme aktuell gehalten und mit Patches versehen werden
- Fördert Wachstum und hilft bei der Entwicklung von Mitarbeiter-Kompetenz
- Vermindert finanzielle Verluste und negative Publicity

8.2.1. Entwickeln einer Methode

Um die Auswahl der richtigen Tools für die Schwachstellenanalyse zu unterstützen, ist es sinnvoll, zuerst eine Methode für die Schwachstellenanalyse zu entwickeln. Es gibt zur Zeit leider keine vordefinierten oder industrieweit bewährten Methoden, jedoch reichen meistens gesunder Menschenverstand und optimale Verfahren als Leitfaden aus.

Was ist das Ziel? Betrachten wir nur einen Server, oder das gesamte Netzwerk und alles innerhalb des Netzwerks? Betrachten wir die Firma intern oder extern? Die Antworten auf diese Fragen sind wichtig, da diese Ihnen bei der Entscheidung über die richtigen Tools und den Einsatz derer helfen.

Weitere Informationen zur Entwicklung von Methoden finden Sie auf den folgenden Webseiten:

- http://www.isecom.org/projects/osstmm.htm — *The Open Source Security Testing Methodology Manual* (OSSTMM)
- http://www.owasp.org/ — *The Open Web Application Security Project*

8.3. Auswerten der Tools

Eine typische Analyse beginnt mit dem Einsatz eines Tools für das Sammeln von Informationen. Bei der Analyse des gesamten Netzwerks sollten Sie zuerst das Layout festlegen, um aktive Hosts zu identifizieren. Sobald diese gefunden wurden, sollten Sie jeden Host einzeln untersuchen. Das Untersuchen dieser Hosts bedarf weiterer Tools. Das Wissen, welche Tools für was verwendet werden, ist der wohl bedeutendste Schritt beim Aufdecken von Schwachstellen.

Wie bei jedem Aspekt des täglichen Lebens gibt es viele verschiedene Tools, die die gleiche Arbeit verrichten. Dies trifft auch auf Schwachstellenanalysen zu. Es gibt Tools, die speziell für Betriebssysteme, Applikationen oder Netzwerke (basierend auf Protokollen) eingesetzt werden können. Einige Tools sind kostenlos, andere wiederum nicht. Einige Tools sind intuitiv und benutzerfreundlich, andere eher kryptisch und schlecht dokumentiert oder besitzen Features, die andere Tools wiederum nicht haben.

Das Finden der richtigen Tools kann eine Herausforderung darstellen. Schlussendlich zählt die Erfahrung. Wenn möglich, richten Sie ein Testlabor ein und probieren soviele Tools aus wie nur möglich, und beachten Sie dabei die Stärken und Schwächen. Lesen Sie die README-Datei oder man-Seite zum Tool. Suchen Sie zusätzlich dazu im Internet nach weiteren Informationen wie Artikel, Schritt-für-Schritt-Anleitungen und Mailinglisten für ein Tool.

Die untenstehend beschriebenen Tools sind nur ein kleines Beispiel der erhältlichen Tools.

8.3.1. Scannen von Hosts mit Nmap

Nmap ist ein beliebtes Tool, das mit Red Hat Enterprise Linux ausgeliefert wird, und zum Feststellen eines Netzwerk-Layouts verwendet werden kann. Nmap ist schon seit vielen Jahren auf dem Markt und ist das wahrscheinlich am häufigsten verwendete Tool für die Sammlung von Informationen. Es enthält eine ausgezeichnete man-Seite, die detaillierte Informationen zu Optionen und Verwendung bietet. Administratoren können Nmap in einem Netzwerk verwenden, um Hosts und offene Ports auf diesen Systemen zu finden.

Nmap ist ein kompetenter, erster Schritt bei der Schwachstellenanalyse. Sie können die Hosts in Ihrem Netzwerk aufzeigen und eine Option angeben, die versucht zu bestimmen, welches Betriebssystem auf einem bestimmten Host läuft. Nmap ist eine gute Grundlage für das Einführen sicherer Services und das Abstellen unbenutzter Services.

8.3.1.1. Nmap verwenden

Nmap kann von einem Shell-Prompt aus verwendet werden. Geben Sie an einem Shell-Prompt den Befehl `nmap` gefolgt vom Hostnamen oder der IP-Adresse des zu scannenden Computers ein.

```
nmap foo.example.com
```

Die Ergebnisse des Scannens (die einige Minuten brauchen können, abhängig davon, wo sich der Host befindet), sollten wie folgt aussehen:

```
Starting nmap V. 3.50 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1591 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
111/tcp    open        sunrpc
443/tcp    open        https
515/tcp    open        printer
950/tcp    open        oftep-rpc
6000/tcp   open        X11

Nmap run completed -- 1 IP address (1 host up) scanned in 71.825 seconds
```

Nmap prüft die häufigsten Ports für die Netzwerkkommunikation auf mithörende oder wartende Services. Dieses Wissen ist sinnvoll für Administratoren, die unnötige Services abschalten möchten.

Weitere Informationen zu Nmap finden Sie auf der offiziellen Homepage unter folgender URL:

http://www.insecure.org/

8.3.2. Nessus

Nessus ist ein Komplett-Service Sicherheitsscanner. Die Plug-In-Architektur von **Nessus** ermöglicht Benutzern das Anpassen an deren Systeme und Netzwerke. Wie mit jedem Scanner ist **Nessus** nur so gut wie die Signatur-Datenbank, die verwendet wird. Glücklicherweise wird **Nessus** häufig aktualisiert und dessen Features beinhalten vollständige Berichterstattung, Host-Scanning und Echtzeit-Schwachstellensuche. Denken Sie jedoch immer daran, dass fehlerhafte Ergebnisse auch bei einem so leistungsstarken und häufig aktualisiertem Tool wie **Nessus** auftreten können.

Hinweis

Nessus wird nicht mit Red Hat Enterprise Linux mitgeliefert und wird nicht unterstützt. Die Erwähnung in diesem Handbuch gilt nur als Referenz für Benutzer, die eventuell an dieser beliebten Applikation interessiert sind.

Weitere Informationen zu Nessus finden Sie auf der offiziellen Homepage unter folgender URL:

http://www.nessus.org/

8.3.3. Nikto

Nikto ist ein ausgezeichneter CGI-Scanner (Common Gateway Interface). Nikto hat die Fähigkeit, nicht nur CGI-Schwachstellen zu suchen, sondern diese auch so zu prüfen, dass Intrusion-Detection-Systeme umgangen werden. Es wird von ausgezeichneter Dokumentation begleitet, die vor dem Ausführen des Programms sorgfältig gelesen werden sollte. Wenn Sie Webserver mit CGI-Skripten besitzen, ist Nikto eine ausgezeichnete Quelle für das Prüfen der Sicherheit dieser Server.

Hinweis

Nikto wird nicht mit Red Hat Enterprise Linux mitgeliefert und wird nicht unterstützt. Die Erwähnung in diesem Handbuch gilt nur als Referenz für Benutzer, die an dieser beliebten Applikation interessiert sind.

Weitere Informationen zu Nikto finden Sie unter folgender URL:

http://www.cirt.net/code/nikto.shtml

8.3.4. VLAD Scanner

VLAD ist ein Schwachstellen-Scanner, der vom RAZOR-Team bei Bindview, Inc. entwickelt wurde und für das Prüfen auf Schwachstellen eingesetzt werden kann. Es prüft laut SANS Top Ten Liste der häufigsten Sicherheitsprobleme (SNMP-Probleme, Datei-Sharing Fragen, etc.). Obwohl er nicht soviele Features wie **Nessus** besitzt, ist VLAD auf jeden Fall wert, genauer betrachtet zu werden.

Hinweis

VLAD wird nicht mit Red Hat Enterprise Linux mitgeliefert und wird nicht unterstützt. Die Erwähnung in diesem Handbuch gilt nur als Referenz für Benutzer, die an dieser beliebten Applikation interessiert sind.

Weitere Informationen zu VLAD finden Sie auf der Webseite des RAZOR-Teams unter folgender URL:

http://www.bindview.com/Support/Razor/Utilities/

8.3.5. Ihre zukünftigen Bedürfnisse vorausplanen

Abhängig von Ihrem Ziel und den Ressourcen gibt es viele Tools auf dem Markt. Es gibt Tools für Wireless Netzwerke, Novell-Netzwerke, Windows Systeme, Linux Systeme und vieles mehr. Einen weiteren, wichtigen Teil der Analysen kann auch die physikalische Sicherheit, Mitarbeiterüberwachung oder Voice/PBX-Netzwerkanalysen sein. Sie können neue Konzepte wie das *War Walking* — das Scannen der Perimeter der physischen Struktur des Unternehmens auf Schwachstellen im Wireless Netzwerk — erforschen und in Ihre Analysen übernehmen. Fantasie und Erfahrung im Umgang mit der Auffindung und Lösung von Sicherheitsproblemen sind die einzigen Grenzen bei der Planung und Durchführung von Schwachstellenanalysen.

IV. Eindringung und Gegenmaßnahmen

Es ist unvermeidbar, dass ein Netzwerk einem Einbruch zur Last fällt oder Netzwerk-Ressourcen missbraucht werden. Dieser Abschnitt spricht pro-aktive Maßnahmen an, die ein Administrator treffen kann, um Sicherheitseinbrüche zu verhindern. Das Einrichten eines IDS (Intrusion Detection System) oder die Formierung eines ER-Teams (Emergency Response), das schnell und effektiv auf Sicherheitsprobleme antworten kann, sind einige solcher Maßnahmen. Dieser Abschnitt beschreibt auch die Schritte, die ein Administrator vornehmen kann, um Beweise eines Sicherheitseinbruchs zu sammeln und auszuwerten.

Inhaltsverzeichnis

9. Intrusion Detection 87
10. Vorfallsreaktion 93

Kapitel 9.

Intrusion Detection

Wertvolle Güter müssen vor Diebstahl und Zerstörung geschützt werden. Einige Häuser sind mit Alarmanlagen ausgerüstet, die Einbrecher abwehren, Behörden nach einem Einbruch benachrichtigen oder sogar die Besitzer bei einem Hausbrand warnen können. Solche Maßnahmen sind notwendig, um die Integrität der Häuser und die Sicherheit der Hausbesitzer zu gewährleisten.

Die gleiche Gewährleistung von Integrität und Sicherheit sollte auch auf Computersysteme und Daten angewandt werden. Das Internet hat den Informationsfluss, von persönlichen bis zu finanziellen Daten möglich gemacht. Zur gleichen Zeit hat es genauso viele Gefahren heraufbeschworen. Böswillige Benutzer und Cracker suchen sich verletzbare Angriffsziele wie ungepatchte Systeme, mit Trojanern infizierte Systeme und Netzwerke mit unsicheren Diensten. Es wird ein Alarm benötigt, der Administratoren und Mitglieder des Sicherheitsteams warnt, dass ein Bruch vorgefallen ist, so dass diese in Echtzeit reagieren können. *Intrusion Detection Systems* wurden als ein solches Alarmsystem entworfen.

9.1. Definition der Intrusion Detection Systeme

Ein Intrusion Detection System (IDS) ist ein aktiver Prozess oder ein aktives Gerät, das die System- und Netzwerkaktivität auf unbefugte Zugriffe und/oder böswillige Aktivitäten analysiert. Die Methode, wie IDS Anomalien entdeckt, kann variieren; das ultimative Ziel einer jeden IDS ist jedoch das Ertappen auf frischer Tat, bevor ernsthafte Schäden am System angerichtet werden.

IDS schützen ein System vor einer Attacke, vor Missbrauch und Kompromittierung. Sie können auch Netzwerkaktivitäten überwachen, Netzwerk- und Systemkonfigurationen auf Schwachstellen prüfen, Datenintegrität analysieren und vieles mehr. Abhängig von der Methode, die Sie einsetzen möchten, gibt es verschiedene direkte und indirekte Vorteile von IDS.

9.1.1. Typen von IDS

Das Verständnis, was ein IDS ist, und welche Funktionen bereitgestellt werden, ist der Schlüssel zu der Entscheidung, welche Art IDS in Ihrer Computersicherheitspolice angemessen ist. In diesem Abschnitt werden die Konzepte hinter IDS, die Funktionalitäten jeder IDS-Art und das Auftauchen hybrider IDS, die mehrere Erkennungstaktiken und Tools in einem Paket integrieren, behandelt.

Einige IDS sind *knowledge-based*, und warnen im voraus Sicherheitsadministratoren vor einem Einbruch mit Hilfe einer Datenbank der häufigsten Attacken. Alternativ dazu gibt es *behavioral-based* (verhaltens-basierte) IDS, die Ressourcen auf Anomalien untersuchen, was meistens ein Zeichen für unbefugte Aktivitäten mit böswilliger Absicht ist. Einige IDS sind Standalone-Dienste, die im Hintergrund arbeiten und passiv auf Aktivitäten abhören und alle verdächtigen Pakete von außen protokollieren. Andere kombinieren Standard-System-Tools, veränderte Konfigurationen und detailliertes Logging mit der Intuition eines Administrators und der Erfahrung, ein leistungsstarkes Einbruch-Erkennungs-Kit zu erstellen. Das Auswerten dieser vielen Intrusion-Detection-Technologien kann Ihnen beim Finden des für Sie richtigen Programms helfen.

Die gängigsten IDS-Arten in Bezug auf Sicherheit sind bekannt als *host-basiert* und *netzwerk-basiert*. Ein host-basiertes IDS ist gleichzeitig das Umfassendste von beiden, was die Implementierung eines Detection-Systems auf jedem individuellen Host umfasst. Dies bedeutet, dass der Host immer geschützt ist, unabhängig von der Netzwerkumgebung. Ein netzwerk-basiertes IDS übertragt die Daten zuerst an eine Einheit, bevor diese an den Zielrechner geschickt werden. Netzwerk-basierte IDS werden meist als unzureichend anerkannt, da viele Rechner in mobilen Umgeben eine zuverlässige Datenflusskontrolle/-überwachung nicht ermöglichen.

9.2. Host-basiertes IDS

Ein *host-basiertes* IDS analysiert verschiedene Gebiete um Missbrauch (Aktivitäten mit böswilliger oder missbräuchlicher Absicht innerhalb des Netzwerks) oder Einbruch (von außen) festzustellen. Host-basierte IDS konsultieren verschiedene Arten von Log-Dateien (Kernel, System, Server, Netzwerk, Firewall und viele mehr) und vergleichen diese Logs mit einer internen Datenbank, die häufige Signaturen bekannter Attacken enthält. Host-basierte IDS für UNIX und Linux machen starken Gebrauch von `syslog` und dessen Fähigkeit, geloggte Vorkommnisse je nach Gewichtigkeit einzuteilen (z.B. geringfügige Drucker-Nachrichten im Vergleich zu wichtigen Kernelwarnungen). Der Befehl `syslog` kann durch die Installation des `sysklogd`-Pakets angewandt werden, welches in Red Hat Enterprise Linux inkludiert ist. Dieses Paket bietet System-Logging und Kernel-Message-Trapping. Die host-basierten IDS filtern Logs (die im Falle einiger Netzwerk- und Kernel-Event-Logs ziemlich detailliert sein können), analysieren diese, versehen die abweichenden Nachrichten mit einem eigenen Kennzeichen je nach Gewichtigkeit des Vorfalles und sammeln diese in einem bestimmten Log für die Analyse durch den Administrator.

Host-basierte IDS können auch die Datenintegrität wichtiger Dateien und die von ausführbaren Programmen prüfen. Eine Datenbank mit wichtigen Dateien (und allen anderen Dateien, die Sie hinzufügen möchten) wird geprüft, und eine *Prüfsumme* jeder Datei über ein Programm wie `md5sum` (128-bit Algorithmus) oder `shalsum` (160-bit Algorithmus) erstellt. Das host-basierte IDS speichert diese Summen in einer Nur-Textdatei und vergleicht in periodischen Abständen die Prüfsummen mit den Werten in der Textdatei. Stimmen die Prüfsummen der Datei nicht überein, warnt das IDS den Administrator per E-Mail oder Mobiltelefon-Pager. Dieser Vorgang wird von Tripwire verwendet, der in Abschnitt 9.2.1 näher beschrieben wird.

9.2.1. Tripwire

Tripwire ist das beliebteste host-basierte IDS für Linux. Tripwire, Inc., die Entwickler von Tripwire, haben vor Kurzem den Software-Quellcode für die Linux-Version geöffnet und unter der GNU General Public License lizenziert. Tripwire ist unter http://www.tripwire.org/ erhältlich.

Hinweis

Tripwire wird nicht mit Red Hat Enterprise Linux ausgeliefert und wird nicht unterstützt. Es wurde in diesem Handbuch als Referenz für Benutzer, die Interesse an der Verwendung dieses Tools haben, gegeben.

9.2.2. RPM als IDS

Der RPM Paket Manager (RPM) ist ein weiteres Programm, das als host-basiertes IDS verwendet werden kann. RPM enthält verschiedene Optionen für das Abfragen von Paketen und deren Inhalt. Diese Verifizierungsoptionen können von unschätzbarem Wert für einen Administrator sein, der im Verdacht hat, dass wichtige Systemdateien und Executables verändert wurden.

Im folgenden finden Sie eine ausführlichere Liste einiger RPM-Optionen, mit denen Sie die Dateiintegrität auf einem Red Hat Enterprise Linux-System verifizieren können. Für eine vollständige Information über die Verwendung von RPM finden Sie im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Wichtig

Einige der Befehle in dieser Liste erfordern das Importieren des Red Hat GPG öffentlichen Schlüssels in Ihren RPM-Schlüsselring. Dieser Schlüssel verifiziert, dass die auf Ihrem System instal-

lierten Pakete eine Paketsignatur von Red Hat enthalten, die sicherstellt, dass Ihre Pakete von Red Hat stammen. Der Schlüssel kann mit dem folgenden Befehl importiert werden (ersetzen Sie *<version>* durch die Version der RPM, die auf Ihrem System installiert sind):

```
rpm --import /usr/share/doc/rpm-<version>/RPM-GPG-KEY
```

`rpm -V` *package_name*

Die Option `-V` verifiziert die Dateien im installierten Paket mit dem Namen *package_name*. Wird keine Ausgabe ausgegeben und das Programm beendet, bedeutet dies, dass keine der Dateien seit dem letzten Update der RPM-Datenbank in irgendeiner Weise geändert wurden. Wird ein Fehler wie z.B. folgender angezeigt,

```
S.5....T c /bin/ps
```

dann wurde die Datei in irgendeiner Weise verändert und Sie sollten überprüfen, ob Sie die Datei behalten wollen (wie z.B. bei geänderten Konfigurationsdateien im Verzeichnis `/etc/`) oder diese Datei löschen und das Paket, das die Datei enthielt, neu installieren möchten. In der folgenden Liste werden die Komponenten des 8-Zeichen-Strings genauer beschrieben (`S.5....T` im Beispiel oben), die einen Verifizierungsfehler bekanntgeben.

- `.` — Der Test hat diese Phase der Verifizierung bestanden
- `?` — Es wurde eine Datei gefunden, die nicht gelesen werden konnte. Dies ist wahrscheinlich ein Problem der Dateiberechtigungen
- `S` — Es wurde eine Datei gefunden, die kleiner oder größer als die ursprünglich auf dem System installierte Datei ist
- `5` — Es wurde eine Datei gefunden, deren md5-Prüfsumme nicht mit der ursprünglichen Prüfsumme dieser Datei übereinstimmt
- `M` — Es wurde ein Fehler in der Dateiberechtigung oder mit dem Typ der Datei gefunden
- `D` — Es wurde ein Übereinstimmungsfehler in der Major/Minor-Nummer der Gerätedateien gefunden
- `L` — Es wurde ein symbolischer Link gefunden, der zu einem anderen Dateipfad weist
- `U` — Es wurde eine Datei gefunden, deren Besitzer geändert wurde
- `G` — Es wurde eine Datei gefunden, deren Gruppenrechte geändert wurden
- `T` — Es wurden `mtime` Verifizierungsfehler in der Datei gefunden

`rpm -Va`

Die Option `-Va` verifiziert *alle* installierten Pakete und findet jegliche Fehler in deren Verifizierungstests (fast genauso wie die Option `-V`, jedoch genauer in der Ausgabe, da jedes installierte Paket verifiziert wird).

`rpm -Vf /bin/ls`

Die Option `-Vf` verifiziert individuelle Dateien in einem installierten Paket. Dies kann sehr hilfreich sein, wenn Sie eine schnelle Verifikation einer verdächtigen Datei durchführen wollen.

`rpm -K` *application-1.0.i386.rpm*

Die Option `-K` ist hilfreich für das Prüfen der md5-Prüfsumme und der GPG-Signatur einer RPM-Paket-Datei. Dies ist sinnvoll, wenn Sie feststellen wollen, ob ein Paket, dass Sie installieren, von Red Hat oder einer anderen Organisation, deren GPG-Schlüssel Sie in Ihrem Schlüsselring

haben, signiert ist. Wurde ein Paket nicht ordnungsgemäß signiert, wird eine Fehlermeldung wie folgende ausgegeben:

```
application-1.0.i386.rpm (SHA1) DSA sha1 md5 (GPG) NOT OK
    (MISSING KEYS: GPG#897da07a)
```

Seien Sie vorsichtig, wenn Sie unsignierte Pakete installieren, da diese nicht von Red Hat, Inc. anerkannt sind und böswilligen Code enthalten können.

RPM kann ein leistungstarkes Tool sein, wie durch die vielen Verifizierungstools für installierte Pakete und RPM-Paket-Dateien. Es wird dringend empfohlen, dass Sie ein Backup des Inhalts Ihres RPM-Datenbank-Verzeichnisses (`/var/lib/rpm/`) auf CD-ROM etc. durchführen, nachdem Sie Red Hat Enterprise Linux installiert haben. Hierdurch können Sie sicher Dateien und Pakete gegen diese Datenbank verifizieren, anstelle die Datenbank auf dem System zu verwenden, da böswillige Benutzer die Datenbank korrumpieren und dadurch Ihre Ergebnisse beeinflussen können.

9.2.3. Andere host-basierte IDS

Im folgenden werden einige der anderen, erhältlichen und beliebten host-basierten Intrusion-Detection-Systme beschrieben. Bitte lesen Sie dazu die Webseiten der jeweiligen Utilities für weitere Informationen zur Installation und Konfiguration.

Hinweis

Diese Applikationen werden nicht mit Red Hat Enterprise Linux ausgeliefert und werden nicht unterstützt. Sie werden in diesem Handbuch als Referenz für Benutzer, die Interesse an der Evaluation dieser Tools haben, gegeben.

- SWATCH http://sourceforge.net/projects/swatch/ — Der Simple WATCHer (SWATCH) verwendet von `syslog` generierte Logdateien zur Warnung vor Anomalien, die auf Benutzerkonfigurationsdateien beruhen. SWATCH wurde entworfen, um jedes Ereignis, das der Benutzer zur Konfigurationsdatei hinzufügen will, aufzuzeichnen. Es wurde jedoch weitestgehend als host-basiertes IDS übernommen.
- LIDS http://www.lids.org/ — Das Linux Intrusion Detection System (LIDS) ist ein Kernel-Patch und ein Administrationstool, das auch Dateiänderungen über Zugangskontrolllisten (ACLs) kontrolliert und Prozesse und Dateien schützt, selbst vor dem root-Benutzer.

9.3. Netzwerk-basierte IDS

Netzwerk-basierte Intrusion-Detection-Systeme funktionieren anders als host-basierte IDS. Die Design-Philosophie eines netzwerk-basierten IDS ist das Scannen von Netzwerkpaketen am Router oder Host, Prüfen von Paket-Informationen und das Logging jeglicher verdächtiger Pakete in einer speziellen Log-Datei mit erweiterten Informationen. Basierend auf diesen verdächtigen Paketen kann ein netzwerk-basiertes IDS deren eigene Datenbank mit Signatur bekannter Netzwerkattacken scannen und einen Gewichtigkeitsgrad für jedes Paket festlegen. Übersteigt der Grad der Gewichtigkeit einen bestimmten Wert, wird eine Warn-E-Mail oder eine Nachricht über Mobil-Pager an die Mitarbeiter des Sicherheitsteams abgeschickt, sodass diese die Art der Anomalie weiter prüfen können.

Netzwerk-basierte IDS werden mit wachsendem Internet immer beliebter. IDS, die große Mengen an Netzwerkaktivitäten scannen und verdächtige Übertragungen erfolgreich mit Tags versehen können,

sind in der Sicherheitsindustrie hoch angesehen. Durch die Unsicherheit des TCP/IP-Protokolls wurde es unumgänglich, Scanner, Schnüffler und andere Netzwerkprüf- und Erkenntools zu entwickeln, die Sicherheitsbrüche durch unter anderem folgende Netzwerkaktivitäten verhindern:

- IP-Spoofing
- Denial-of-Service Attacken
- arp Cache-Poisoning
- DNS-Name-Korruption
- Man-in-the-Middle Attacken

Die meisten netzwerk-basierten IDS erfordern, dass das Netzwerkgerät des Hostsystems auf *Promiscuous* gesetzt wird, was dem Gerät erlaubt, *jedes* Paket im Netzwerk abzufangen. Der Promiscuous-Moduskann durch den Befehl `ifconfig` z.B. wie folgt gesetzt werden:

```
ifconfig eth0 promisc
```

Das Ausführen von `ifconfig` ohne Optionen zeigt, dass `eth0` sich nun im Promiscuous-Modus (`PROMISC`) befindet.

```
eth0      Link encap:Ethernet  HWaddr 00:00:D0:0D:00:01
          inet addr:192.168.1.50  Bcast:192.168.1.255  Mask:255.255.252.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:6222015 errors:0 dropped:0 overruns:138 frame:0
          TX packets:5370458 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2505498554 (2389.4 Mb)  TX bytes:1521375170 (1450.8 Mb)
          Interrupt:9 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:21621 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21621 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1070918 (1.0 Mb)  TX bytes:1070918 (1.0 Mb)
```

Durch das Verwenden eines Tools wie `tcpdump` (mit Red Hat Enterprise Linux ausgeliefert) können wir den Verkehr im Netzwerk sehen:

```
tcpdump: listening on eth0
02:05:53.702142 pinky.example.com.ha-cluster > \
 heavenly.example.com.860:  udp 92 (DF)
02:05:53.702294 heavenly.example.com.860 > \
 pinky.example.com.ha-cluster:  udp 32 (DF)
02:05:53.702360 pinky.example.com.55828 > dns1.example.com.domain: \
 PTR? 192.35.168.192.in-addr.arpa. (45) (DF)
02:05:53.702706 ns1.example.com.domain > pinky.example.com.55828: \
 6077 NXDomain* 0/1/0 (103) (DF)
02:05:53.886395 shadowman.example.com.netbios-ns > \
 172.16.59.255.netbios-ns: NBT UDP PACKET(137): QUERY; BROADCAST
02:05:54.103355 802.1d config c000.00:05:74:8c:a1:2b.8043 root \
 0001.00:d0:01:23:a5:2b pathcost 3004 age 1 max 20 hello 2 fdelay 15
02:05:54.636436 konsole.example.com.netbios-ns > 172.16.59.255.netbios-ns:\
 NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
02:05:56.323715 pinky.example.com.1013 > heavenly.example.com.860:\
 udp 56 (DF)
02:05:56.323882 heavenly.example.com.860 > pinky.example.com.1013:\
 udp 28 (DF)
```

Beachten Sie, dass die Pakete, die nicht für unseren Computer bestimmt waren (`pinky.example.com`), noch von `tcpdump` gescannt und geloggt werden.

9.3.1. Snort

Auch wenn `tcpdump` ein nützliches Prüftool darstellt, wird es nicht als wahres IDS betrachtet, da es Pakete nicht auf Anomalien analysiert und markiert. `tcpdump` druckt *alle* Paketinformationen auf dem Ausgabebildschirm oder in einer Logdatei, ohne Analyse oder Ausarbeitung. Ein richtiges IDS analysiert die Pakete, markiert potentiell schädliche Pakete und speichert diese in einem formatierten Log.

Snort ist ein IDS, das für umfassendes und akkurates Logging von böswilligen Netzwerkaktivitäten und Benachrichtigung von Administratoren bei potentiellen Brüchen entwickelt wurde. Snort verwendet die Standard-`libcap`-Bibliothek und `tcpdump` als Paket-Logging-Backend.

Das beste Feature von Snort, zusätzlich zur Funktionalität, ist das flexible Attacken-Signatur-Subsystem. Snort hat eine ständig aktualisierte Attacken-Datenbank, die über das Internet ergänzt und aktualisiert werden kann. Benutzer können Signaturen basierend auf Netzwerkattacken erstellen und diese an die Snort-Signatur-Mailinglisten weitergeben (unter http://www.snort.org/lists.html), sodass alle Benutzer von Snort hiervon profitieren. Diese Ethik der Community, Informationen zu teilen, hat Snort zu einem der aktuellsten und robustesten netzwerk-basierten IDS gemacht.

Hinweis

Snort wird nicht mit Red Hat Enterprise Linux ausgeliefert und wird nicht unterstützt. Es wurde in diesem Handbuch als Referenz für Benutzer, die Interesse an der Evaluation dieses Tools haben, gegeben.

Weitere Informationen zu Snort finden Sie auf der offiziellen Webseite unter http://www.snort.org/.

Kapitel 10.

Vorfallsreaktion

Im Falle, dass das die Sicherheit eines Systems kompromittiert wurde, ist eine *Vorfallsreaktion* notwendig. Es liegt in der Verantwortung des Sicherheitsteams, schnell und effektiv auf das Problem zu reagieren.

10.1. Definition der Vorfallsreaktion

Vorfallsreaktion ist eine Express-Reaktion auf ein sicherheitsbezogenens Problem oder einen Vorfall. In Bezug auf Informationssicherheit wäre dies z.B. das Vorgehen eines Sicherheitsteams gegen einen Hacker, der eine Firewall durchdrungen hat und nun das interne Netzwerk auskundschaftet. Dieser Vorfall ist ein Sicherheitsbruch. Die Reaktion hängt vom Sicherheitsteam ab, was diese tun, um den Schaden gering zu halten und wann die Ressourcen wiederhergestellt werden, während die Datenintegrität weiterhin aufrechterhalten wird.

Denken Sie an Ihr Unternehmen, und wie fast alles sich auf Technologie und Computersysteme verlässt. Wird dies kompromittiert, stellen Sie sich die möglichen, verheerenden Schäden vor. Abgesehen von einem Systemausfall und Datendiebstahl könnten Daten korrumpiert werden, Identitätendiebstahl kann auftreten (durch Online-Personalakten), und peinliche Publicity oder sogar finanzieller Ruin kann die Folge sein, wenn Kunden und Geschäftspartner von einem Sicherheitsbruch erfahren und negativ reagieren.

Untersuchungen vergangener Sicherheitsverletzungen (intern und extern) haben gezeigt, dass Firmen als Folge eines Sicherheitsbruches bankrott gehen können. Ein Sicherheitsbruch kann Ressourcen unverfügbar machen, oder zu Diebstahl oder Korruption von Daten führen. Man sollte auch nicht diejenigen Dinge vernachlässigen, die vom finanziellen Aspekt her schwer zu kalkulieren sind, wie z.B. schlechte Publicity. Ein Unternehmen muss die Kosten eines Sicherheitsbruches kalkulieren und die negativen Auswirkungen auf das Unternehmen kurz- und langfristig einschätzen können.

10.2. Erstellen eines Incident-Response-Plans

Es ist wichtig, das ein *Vorfallsreaktionsplan* formuliert, im gesamten Unternehmen unterstützt, in die Tat umgesetzt und regelmäßig getestet wird. Ein guter Vorfallsreaktionsplan kann die Auswirkungen einer Sicherheitsverletzung minimieren. Desweiteren kann er negative Publicity reduzieren.

Aus der Perspektive eines Sicherheitsteams ist es nicht wichtig, ob ein Verstoß auftritt (da solche Vorkommnisse ein vorherzusehender Teil der Verwendung eines vertrauensunwürdigen Trägernetzwerks wie das Internet sind), sondern *wann* dieses Vergehen auftritt. Denken Sie nicht, das ein System grundsätzlich schwach und anfällig ist, sondern machen Sie sich klar, dass mit genügend Zeit und Ressourcen jemand selbst in das sicherste System oder Netzwerk einbrechen kann. Besuchen Sie doch einmal die *Security Focus* Webseite unter http://www.securityfocus.com/ für aktuelle und detaillierte Informationen zu neuesten Sicherheitsbrüchen und Anfälligkeiten, von der häufigen Verunstaltung von Firmenwebseiten bis hin zum legendären Angriff auf die Root-DNS-Nameserver im Jahre 2002[1].

Der positive Aspekt der Erkenntnis, dass einer Systemverletzung unvermeidbar ist, ist derjenige, dass das Sicherheitsteam einen Aktionsplan entwickeln kann, der mögliche Schäden verringert. Die Kombination eines Aktionsplans mit Kompetenz ermöglicht dem Team, auf widrige Umstände formell zu reagieren.

Der Vorfallsreaktionsplan kann in vier Phasen unterteilt werden:

1. http://www.gcn.com/21_32/web/20404-1.html

- Sofortige Aktion, um den Vorfall zu stoppen oder zu minimieren
- Untersuchen des Vorfalls
- Wiederherstellung von betroffenen Ressourcen
- Melden des Vorfalls an die richtigen Stellen

Eine Vorfallsreaktion muss entschieden und schnell ausgeführt werden. Sie lässt in den meisten Fällen wenig Raum für Fehler. Dadurch, das Notfälle geprobt und die Reaktionszeiten gemessen werden, ist es möglich, eine Methodologie zu entwickeln, die Schnelligkeit und Exaktheit fördert. Eine schnelle Reaktion kann die Auswirkung auf Ressourcen und mögliche Schäden im Ernstfall verringern.

Ein Vorfallsreaktionsplan hat eine Anzahl von Anforderungen, inklusive:

- Einem Team von In-House Experten (ein *Computer Emergency Response Team*)
- Einer rechtlich abgesicherten und genehmigten Strategie
- Finanzieller Unterstützung durch das Unternehmen
- Unterstützung durch den Vorstand oder die obere Führungsebene
- Eines durchführbaren und getesteten Aktionsplans
- Physikalischer Ressourcen wie Extra-Speicher, Standby-Systeme und Backup-Services

10.2.1. Ein Computer Emergency Response Team (CERT)

Ein Computer Emergency Response Team (CERT) (zu deutsch: Computer-Notfall-Reaktions-Team) ist eine Gruppe von In-House Experten, die im Falle einer Computer-Katastrophe schnell handeln können. Die Kernkompetenzen für ein CERT zu definieren, kann eine Herausforderung darstellen. Das Konzept von angemessenem Personal geht über die technische Kompetenz hinaus und umfasst logistische Faktoren wie Ort, Verfügbarkeit und die Einstellung, das Unternehmen im Notfall allem voran zu stellen. Ein Notfall tritt niemals geplant auf; er kann jeden Moment eintreten, und alle CERT-Mitglieder müssen dann die von ihnen verlangte Verantwortung übernehmen, auf einen Notfall zu jeder Zeit zu reagieren.

Typische CERT-Mitglieder sind z.B. System- und Netzwerkadministratoren sowie Mitglieder der Informationssicherheitsabteilung. Systemadministratoren liefern das Wissen und die Erfahrung in Bezug auf die Systemressourcen inklusive Daten-Backups, vorhandene Backup-Hardware und vieles mehr. Netzwerkadministratoren liefern deren Wissen über Netzwerkprotokolle und die Fähigkeit, Netzwerk-Verkehr dynamisch umzuleiten. Informationssicherheitspersonal ist hilfreich für das genaueste Verfolgen von Sicherheitsproblemen und eine *Post-Mortem*-Analyse (nach dem Angriff) kompromittierter Systemen.

Es ist nicht immer tragbar, aber es sollte ein gewisser Personalüberschuss innerhalb eines CERT bestehen. Sind tiefergehende Kompetenzen nicht auf ein Unternehmen anwendbar, sollte zumindest Cross-Training durchgeführt werden. Denken Sie daran, dass wenn nur eine Person den Schlüssel zu Datensicherheit und Integrität besitzt, das gesamte Unternehmen hilflos wird, falls diese Person abwesend ist.

10.2.2. Rechtliche Betrachtungen

Einige wichtige Aspekte einer Vorfallsreaktion, die betrachtet werden müssen, sind rechtliche Angelegenheiten. Sicherheitspläne sollten zusammen mit Mitarbeitern der Rechtsabteilung oder einer allgemeinen Form von Rechtsbeistand erarbeitet werden. Genauso wie jede Firma eine eigene Sicherheitspolice im Unternehmen haben sollte, so sollte jedes Unternehmen seine eigene Methode, Vorfälle vom rechtlichen Standpunkt aus zu behandeln, haben. Regionale, landesweite oder bundesweite Gesetze würden den Rahmen dieses Handbuchs sprengen, werden jedoch kurz angerissen, da die Methodologie für eine Post-Mortem-Analyse zumindest teilweise von rechtlicher Seite aus vorgegeben wird.

Die Rechtsabteilung kann die technischen Mitarbeiter über die Auswirkungen von Sicherheitsverletzungen, die Gefahren der Verbreitung von Kundendaten (persönliche, gesundheitliche oder finanzielle Daten) und die Wichtigkeit, den Service in unternehmenskritischen Umgebungen wie Krankenhäuser oder Banken wiederherzustellen, aufklären.

10.3. Implementieren des Incident-Response-Plans

Nachdem ein Schlachtplan erstellt wurde, muss dieser verabschiedet und aktiv implementiert werden. Jeder Aspekt dieses Plans, der während der Implementierung in Frage gestellt wird, resultiert wahrscheinlich in langsamer Reaktionszeit und Systemausfall, falls ein Verstoß vorliegt. Hier wird praktische Übung unschätzbar. Solange nicht etwas bemängelt wird, bevor der Plan aktiv in der Produktionsumgebung eingesetzt wird, sollte der Plan von allen direkt betroffenen Parteien verabschiedet und zuversichtlich implementiert werden.

Wird ein Bruch bemerkt während die CERT für eine schnelle Reaktion vor-Ort ist, können mögliche Reaktionen variieren. Das Team kann sich einigen, das Netzwerk zu trennen, die betroffenen Systeme zu trennen, das Sicherheitsloch mit einem Patch zu versehen und schnell wieder ohne weitere Komplikationen zu verbinden. Das Team kann auch die Eindringlinge überwachen und deren Aktionen verfolgen. Das Team kann sogar einen Eindringling an einen *Honigtopf* weiterleiten — ein System oder Netzwerksegment, das absichtlich falsche Daten enthält — um den Vorfall sicher zu verfolgen ohne Produktionsressourcen zu unterbrechen.

Die Reaktion auf einen Vorfall sollte, wenn immer möglich, von Informationssammlung begleitet werden. Das Ausführen von Prozessen, Netzwerkverbindungen, Dateien, Verzeichnissen und vielem mehr sollte aktiv in Echtzeit überprüft werden. Ein Schnappschuss der Produktionsressourcen zum Vergleich ist hilfreich beim Verfolgen von schlechten Services oder Prozessen. CERT-Mitglieder und In-House Experten stellen großartige Ressourcen bei der Verfolgung dieser Anomalien in einem System dar. Systemadministratoren wissen, welche Prozesse erscheinen sollten und welche nicht, wenn die Befehle `top` oder `ps` ausgeführt werden. Netzwerkadministratoren wissen, wie normaler Netzwerkverkehr aussieht, wenn `snort` oder `tcpdump` ausgeführt wird. Diese Team-Mitglieder kennen ihre Systeme und sollten in der Lage sein, Anomalien schneller zu entdecken als jemand, der sich mit der Infrastruktur nicht auskennt.

10.4. Untersuchen des Vorfalls

Das Untersuchen einer Computerverletzung ist wie das Untersuchen eines Tatortes. Kriminalbeamte sammeln Beweise, bemerken verdächtige Hinweise und notieren Verluste und Schäden. Eine Analyse einer Computerverletzung kann entweder noch während der Attacke geschehen oder *post-mortem* (nach dem Verstoß).

Obwohl man System-Logdateien auf einem angegriffenen System nicht trauen kann, gibt es kriminaltechnische Utensilien, die Ihnen bei der Analyse helfen. Der Zweck und die Features dieser Tools variieren, aber allgemein erstellen diese Bit-Image-Kopien der Medien, fassen Ereignisse und Prozesse zusammen, zeigen detaillierte Dateisysteminformationen und stellen gelöschte Dateien wo möglich wieder her.

Es ist auch ratsam, alle durchgeführten Untersuchungen auf einem kompromittierten System aufzuzeichnen, in dem Sie den Befehl `script` wie im folgenden Beispiel verwenden:

```
script -q <file-name>
```

Ersetzen Sie *<file-name>* mit dem Dateinamen für das `script`-Log. Speichern Sie die Log-Datei immer auf einem anderem Medium als die Festplatte des kompromittierten Systems — ein Diskette oder eine CD-ROM sind bewährte Medien für diesen Zweck.

Indem Sie Ihre Aktionen aufzeichnen, wird ein Audit-Trail erstellt, der wertvoll sein kann, falls der Angreifer gefasst wird.

10.4.1. Erstellen eines Images als Beweis

Das Erstellen einer Bit-Image Kopie der Medien ist ein sinnvoller erster Schritt. Wenn wir Daten untersuchen, ist dies eine Anforderung. Es wird empfohlen, zwei Kopien zu erstellen Eine für die Analyse und Untersuchung, und eine zweite Kopie, die zusammen mit dem Original gespeichert wird und als Beweismittel in jeglichen rechtlichen Verfahren gilt.

Sie können den Befehl `dd`, der Teil des `coreutils`-Pakets in Red Hat Enterprise Linux ist, verwenden, um ein monolithisches Abbild eines kompromittierten Systems zu erstellen und dies als Beweis in einer Untersuchung oder für den Vergleich mit vertrauenswürdigen Images zu verwenden. Nehmen Sie an, es besteht eine einzelne Festplatte in einem System, von dem Sie ein Abbild machen möchten. Fügen Sie diese Festplatte als Slave zu Ihrem System hinzu und verwenden Sie den Befehl `dd`, um eine Image-Datei zu erstellen:

```
dd if=/dev/hdd bs=1k conv=noerror,sync of=/home/evidence/image1
```

Dieser Befehl erstellt eine einzige Datei mit dem Namen `image1` und verwendet einen 1K Block aus Geschwindigkeitsgründen. Die Option `conv=noerror, sync` zwingt`dd` dazu, mit dem Lesen und Ablegen von Daten fortzufahren, auch wenn defekte Sektoren auf dem verdächtigen Laufwerk gefunden werden. Jetzt können Sie die resultierende Image-Datei studieren oder versuchen, gelöschte Dateien wiederherzustellen.

10.4.2. Post-Breach-Informationen sammeln

Das Thema digitale Untersuchungen und Analysen ist relativ breitgefächert, dennoch sind die Tools ziemlich Architektur-spezifisch und können nicht allgemein angewendet werden. Vorfallsreaktion, Analyse und Wiederherstellung sind jedoch wichtige Themen. Mit dem richtigen Wissen und der Erfahrung wird Red Hat Enterprise Linux zu einer ausgezeichneten Plattform für solche Arten von Analysen, da es verschiedene Utilities für die Rückantwort nach einem Verstoß und für die Wiederherstellung bietet.

Tabelle 10-1 beschreibt im Detail einige Befehle für das Prüfen und Verwalten von Dateien. Es werden außerdem einige Beispiele aufgelistet, die Sie zum richtigen Identifizieren von Dateitypen und Dateiattributen (wie z.B. Berechtigungen und Zugangsdaten) benötigen, so dass Sie weitere Beweise für die Analyse sammeln können. Diese Tools, kombiniert mit Intrusion Detection Systemen, Firewalls, gehärtete Services und andere Sicherheitsmaßnahmen, können potentielle Schäden bei einer Attacke reduzieren.

Hinweis

Detaillierte Informationen über jedes Tool finden Sie auf den jeweiligen man-Seiten.

Befehl	Funktion	Beispiel

Befehl	Funktion	Beispiel
`dd`	Erstellt eine Bit-Image Kopie (oder *disk dump*) von Dateien und Partitionen. Kombiniert mit einer Prüfung der md5sums von jedem Image können Administratoren ein Image der Partition oder der Datei vor dem Bruch mit einem Image, das nach dem Bruch erstellt wurde, vergleichen und prüfen, ob die Prüfsummen übereinstimmen.	`dd if=/bin/ls of=ls.dd |md5sum ls.dd >ls-sum.txt`
`grep`	Findet nützliche (Text)-Informationen innerhalb von Dateien und Verzeichnissen wie zum Beispiel Berechtigungen, Dateiattribute, Skriptänderungen und vieles mehr. Wird hauptsächlich als Pipe-Befehl eines anderen Befehls wie `ls`, `ps` oder `ifconfig` verwendet	`ps auxw |grep /bin`
`strings`	Druckt Ketten druckbarer Zeichen in einer Datei aus. Dies ist sehr nützlich für das Prüfen von ausführbaren Dateien auf Anomalien wie z.B. `mail`-Befehle an unbekannte Adressen oder das Loggen in einer Nicht-Standard-Logdatei.	`strings /bin/ps |grep 'mail'`
`file`	Legt die Charakteristiken von Dateien basierend auf Format, Kodierung, Bibliotheken die verknüpft werden (falls vorhanden) und Dateityp (binär, Text, etc.) fest. Es ist nützlich für das Feststellen, ob eine ausführbare Datei wie `/bin/ls` mittels statischen Bibliotheken geändert wurde, was ein sicheres Zeichen dafür ist, das die ausführbare Datei durch eine von einem Benutzer mit böswilliger Absicht installierte Datei ersetzt wurde.	`file /bin/ls`
`find`	Durchsucht Verzeichnisse auf bestimmte Dateien. Es ist ein nützliches Tool für das Durchsuchen der Verzeichnisstruktur nach Schlüsselwörtern, Datum und Zeit des Zugangs, Berechtigungen, und so weiter. Dies ist nützlich für Administratoren, die allgemeine Systemprüfungen für Verzeichnisse oder Dateien durchführen.	`find -atime +12 -name *log* -perm u+rw`

Befehl	Funktion	Beispiel
`stat`	Zeigt verschiedene Informationen über eine Datei an, inklusive Zeitpunkt des letzten Zugriffs, Berechtigungen, UID und GID-Einstellungen und vieles mehr. Dies kann nützlich für das Prüfen sein, wann eine ausführbare Datei in einem betroffenen System zuletzt verwendet und/oder verändert wurde.	`stat /bin/netstat`
`md5sum`	Berechnet die 128-Bit Prüfsummen mit dem md5-Hash-Algorithmus. Sie können diesen Befehl verwenden, um eine Textdatei mit einer Liste aller wichtigen Executables, die bei einem Systemeinbruch verändert oder ersetzt werden könnten, zu erstellen. Leiten Sie die Summen in eine Datei um, um eine einfache Datenbank mit Prüfsummen zu erhalten, und kopieren Sie dann die Datei auf ein Medium nur mit Leseberechtigung, wie z.B. CD-ROM.	`md5sum /usr/bin/gdm >>md5sum.txt`

Tabelle 10-1. Datei-Prüf-Tools

10.5. Wiederherstellen von Ressourcen

Während eine Vorfallsreaktion ausgeführt wird, sollte das CERT-Team auf Daten- und Systemwiederherstellung hinarbeiten und diese untersuchen. Es liegt jedoch in der Natur der Sicherheitsverletzung, wie bei der Wiederherstellung zu verfahren ist. Backups oder redundante Systeme offline zu haben, hat sich in dieser Situation als unermesslich wertvoll erwiesen.

Um Systeme wiederherzustellen, muss das Team jegliche ausgefallenen Systeme oder Applikationen wie z.B. Authentifitzierungsserver, Datenbankserver und alle anderen Produktionsressourcen wieder online bringen.

Es wird dringend empfohlen, Backup-Hardware für die Produktion einsatzbereit zu haben. Dies umfasst Extra-Festplatten, Ersatz-Server und Ähnliches. Fertige Systeme sollten bereits alle Software geladen haben und für sofortigen Einsatz bereit sein. Es müssen dann vielleicht nur die allerneuesten Daten importiert werden. Dieses fertige System sollte isoliert vom potentiell betroffenen Netzwerk gehalten werden. Tritt ein Sicherheitsbruch auf und das Backup-System ist Teil des Netzwerks, ist es zwecklos, überhaupt ein Backup-System anzulegen.

Systemwiederherstellung ist ein umständlicher Prozess. In vielen Situationen gibt es zwei Methoden, aus denen man auswählen muss. Administratoren können entweder das Betriebssytem neu installieren, gefolgt von einer Neuinstallation aller Applikationen und Daten oder alternativ dazu kann der Administrator das System auch mit einem Patch versehen und das betroffene System wieder zur Produktion zurückbringen.

10.5.1. Neuinstallieren des Systems

Das Durchführen einer sauberen Neuinstallation versichert, dass das betroffene System von allen Trojanern, Backdoors und böswilligen Prozessen gereinigt wird. Eine Neuinstallation stellt außerdem sicher, dass jegliche Daten (wenn von einer vertrauenswürdigen Quelle wiederhergestellt) von böswilligen Veränderungen gereinigt werden. Der Nachteil einer vollständigen Systemwiederherstellung ist der Zeitaufwand, das System von Grund auf neu aufzubauen. Wenn jedoch ein *aktuelles* Backup-System vorhanden ist, bei dem Sie nur die neuesten Daten hinzufügen müssen, wird die Systemausfallzeit erheblich verringert.

10.5.2. Das System mit Patches versehen

Die zweite Möglichkeit ist, die betroffenen Systeme mit einem Patch zu versehen. Diese Wiederherstellungsmethode ist risikoreicher und sollte nur mit großer Vorsicht durchgeführt werden. Die Gefahr eines Patches anstelle einer Neuinstallation ist das Feststellen, ob Sie das System ausreichend von Trojanern, Sicherheitslöchern und korrupten Daten *gereinigt* haben. Wenn Sie einen modularen Kernel verwenden, kann das Patchen eines Systems noch wesentlich schwieriger werden. Die meisten *rootkits* (Programme oder Pakete, die ein Cracker hinterlässt, um Root-Zugang zu Ihrem System zu erhalten), trojanische Systembefehle und Shell-Umgebungen wurden so entwickelt, dass ihre boswilligen Aktivitäten bei Prüfungen nicht gefunden werden. Verwenden Sie die Patch-Methode, sollten nur vertrauenswürdige Binaries (wie zum Beispiel von einer Nur-Lese-CD-ROM) verwendet werden.

10.6. Den Vorfall melden

Der letzte Teil des Incident-Response-Plans ist das Melden des Vorfalls. Das Sicherheitsteam sollte sich während des Vorfalls Notizen machen, um den Vorfall dann Organisationen wie den örtlichen oder bundesweiten Behörden oder herstellerübergreifenden Sicherheitsportals wie die Common Vulnerabilities and Exposures Site (CVE) unter http://cve.mitre.org/ zu melden. Abhängig von der Art des Rechtsbeistandes, den Ihr Unternehmen hat, ist u.U. eine Post-Mortem-Analyse erforderlich. Auch wenn dies keine funktionale Anforderung einer Analyse ist, kann eine Post-Mortem-Analyse doch wertvolle Informationen dazu liefern, wie der Cracker denkt und wie Ihre Systeme strukturiert sind, um zukünftige Probleme zu verhindern.

V. Anhänge

Dieser Abschnitt spricht einige der am häufigsten verwendeten Wege an, in denen ein Eindringling in Ihr System einbrechen kann, oder Ihre Daten während der Übertragung abfangen kann. Dieser Abschnitt beschreibt auch einige der am häufigsten verwendeten Services und deren entsprechenden Port-Nummern, was für einen Administrator, der die Risiken eines Einbruchs vermindern will, nützlich ist.

Inhaltsverzeichnis

A. Hardware- und Netzwerkschutz 103
B. Häufige Schwachstellen und Attacken 109
C. Häufige Ports 113

Anhang A.

Hardware- und Netzwerkschutz

Der beste Ansatz vor dem Einsatz einer Maschine in einer Produktionsumgebung oder dem Verbinden Ihres Netzwerks mit dem Internet ist, die Bedürfnisse Ihres Unternehmens festzulegen und festzustellen, wie Sicherheit in die Anforderungen so transparent wie möglich passt. Da das Hauptziel des *Red Hat Enterprise Linux Sicherheitshandbuch* ist, zu erklären, wie Red Hat Enterprise Linux sicherer gestaltet werden kann, sprengt eine detailierte Untersuchung der Hardware und der physikalischen Netzwerksicherheit den Rahmen dieses Dokuments. Dieses Kapitel liefert jedoch einen kurzen Überblick über das Einrichten von Sicherheitsrichtlinien im Hinblick auf Hardware und physikalische Netzwerke. Wichtige Faktoren sind u.a. wie Computing-Bedürfnisse und Konnektivität in die Gesamt-Sicherheitsstrategie passen. Im Folgenden werden einige der Faktoren im Detail behandelt.

- *Computing* beinhaltet mehr als nur Workstations, auf denen Desktop-Software läuft. Moderne Unternehmen erfordern massive Rechnerleistungen und hochverfügbare Dienste, die z.B. Mainframes, Computer- oder Applikationscluster, leistungsstarke Workstations und spezialisierte Geräte umfassen können. Mit all diesen Anforderungen kommt jedoch auch eine erhöhte Anfälligkeit für Hardware-Ausfälle, Naturkatastrophen und Diebstahl der Ausrüstung.
- *Konnektivität* ist die Methode, mit der ein Administrator ungleichartige Ressourcen auf einem Netzwerk zu verbinden versucht. Ein Administrator verwendet eventuell ein Ethernet (Hub oder Switch CAT-5/RJ-45-Kabel), Token Ring, 10-base-2 Koaxialkabel oder sogar Wireless (802.11x) Technologien. Abhängig vom gewählten Medium erfordern bestimmte Medien und Netzwerktopologien komplementäre Technologien wie z.B. Hubs, Router, Switches, Base Stations und Access Points. Das Festlegen einer funktionalen Netzwerkarchitektur ermöglicht einen leichteren Verwaltungsaufwand, sollten Sicherheitsprobleme auftreten.

Durch diese allgemeinen Überlegungen kann ein Administrator eine bessere Übersicht über die Implementierung erhalten. Das Design einer Computer-Umgebung kann auf den Unternehmens-Anforderungen und Sicherheitsbetrachtungen basieren — eine Implementierung, die beides berücksichtigt.

A.1. Sichere Netzwerktopologien

Das Grundgerüst eines LAN ist die *Topologie* oder Netzwerkarchitektur. Eine Topologie ist das physikalische und logische Layout eines LAN inBezug auf die Ressourcen, Entfernung zwischen Knoten und Übertragungsmedium. Abhängig von den Bedürfnissen des Unternehmens, die das Netzwerk bedient, gibt es mehrere Möglichkeiten für eine Netzwerk-Implementierung. Jede Topologie hat einzigartige Vorteile und wirft Sicherheitsfragen auf, die Netzwerkarchitekten bei der Entwicklung des Netzwerklayouts berücksichtigen sollten.

A.1.1. Physische Topologien

Wie durch das Institute of Electrical and Electronics Engineers (IEEE) festgelegt, gibt es drei allgemeine Topologien für die physikalische Verbindung eines LAN.

A.1.1.1. Ring-Topologie

Die *Ring*-Topologie verbindet jeden Knoten durch genau zwei Verbindungen. Dies erstellt eine Ringstruktur, in der jeder Knoten durch einen anderen zugängig ist. Dies geschieht entweder direkt durch die Nachbarknoten oder indirekt durch den Ring. Token Ring-, FDDI- und SONET-Netzwerke sind auf diese Weise verbunden (FDDI verwendet darüberhinaus eine Doppel-Ring-Technik); es gibt jedoch keine allgemeinen Ethernet-Verbindungen, die diese physikalische Topologie einsetzen. Aus

diesem Grund werden Ringe allgemein eher selten verwendet, außer als Vermächtnis oder auf Institutionellen Systemen mit einer großen Anzahl von Knoten (z.B. eine Universität).

A.1.1.2. Lineare Bus Topologie

Die *Linear Bus* Topologie besteht aus Knoten, die mit einem linearen Kabel, das mit Endwiderständen abgeschlossen ist (Backbone), verbunden sind. Die Linear Bus Topologie benötigt die wenigsten Kabel und Netzwerkausrüstung, und lässt dies somit zur kosteneffektivsten Lösung werden. Der Liner Bus ist jedoch von der ständigen Verfügbarkeit des Backbone abhängig und wird so zu einem einzigen Ausfallpunkt, falls dieser offline genommen werden muss oder die Leitung gekappt wird. Linear Bus Topologien werden häufig in Peer-to-Peer LANs mit Koaxialkabeln und 50 Ohm Endwiderständen an beiden Enden des Buses eingesetzt.

A.1.1.3. Stern-Topologie

Die *Stern*-Topologie besteht aus einem zentralen Punkt, an den die Knoten angeschlossen sind und durch den die Kommunikation weitergeleitet wird. Dieser zentrale Punkt, als *Hub* bezeichnet, kann entweder *broadcasted* oder *switched* sein. Diese Topologie führt zu einem einzigen Schwachpunkt in der zentralisierten Netzwerkhardware, die die Knoten verbindet. Durch diese Zentralisierung sind jedoch Netzwerkprobleme, die entweder Teile des LAN oder das gesamte LAN beeinträchtigen, leicht auf diese eine Fehlerquelle zurückzuführen.

A.1.2. Übertragungs-Betrachtungen

Abschnitt A.1.1.3 stellte das Konzept des Broadcast-Networking und Switched-Networking vor. Es gibt mehrere Faktoren, die bei der Auswahl der Art von Netzwerk-Hardware, die geeignet und sicher für Ihre Netwerkumgebung sein muss, beachtet werden müssen. Das Folgende kennzeichnet diese eindeutigen Arten des Netzwerbetriebes.

In einem Broadcast-Netzwerk sendet ein Knoten ein Paket, das durch jeden Knoten geht, bis der Empfänger das Paket annimmt. Jeder Knoten im Netzwerk kann dieses Datenpaket empfangen bis der Empfänger dieses verarbeitet. In einem Broadcast-Netzwerk werden alle Pakete auf diese Weise gesendet.

In einem Switch-Netzwerk werden Pakete nicht weitergeleitet, sondern in einer Switched Hub verarbeitet, die dann wiederum eine *direkte* Verbindung zwischen den Sender- und Empfängerknoten über Unicast-Übertragungsprinzipien herstellt. Dies eliminiert die Notwendigkeit, Pakete über jeden Knoten zu senden und verringert so das Verkehrsaufkommen.

Das Switched-Netzwerk verhindert außerdem ein Abfangen von Paketen durch bösartige Knoten oder Benutzer. In einem Broadcast-Netzwerk, in dem jeder Knoten ein Paket auf dem Weg zum Zielempfänger erhält, können bösartige Benutzer deren Ethernet-Gerät in den *Promiscuous*-Modus versetzen und alle Pakete annehmen, egal ob die Daten für diesen bestimmt sind oder nicht. Im Promiscuous-Modus kann eine Sniffer-Applikation zum Filtern, Analysieren und Rekonstruieren von Paketen für Passwörter, persönliche Daten und mehr verwendet werden. Fortgeschrittene Sniffer-Applikationen können solche Informationen in Textdateien speichern, und diese eventuell an willkürliche Quellen (z.B. die E-Mail-Adresse des Angreifers) senden.

Ein Switched-Netzwerk benötigt einen Netzwerk-Switch, eine besondere Hadrwarekomponente, die den Platz einer traditionellen Hub, in der alle Knoten auf einem LAN verbunden sind, einnimmt. Switches speichern MAC-Adressen aller Knoten innerhalb einer internen Datenbank, die dann für ein direktes Routing verwendet wird. Verschiedene Hersteller, inklusive Cisco Systems, Linksys und Netgear bieten mehrere Arten von Switches mit Eigenschaften wie 10/100-Base-T Kompatibilität, Gigabit-Ethernet-Support und IPv6-Networking an.

A.1.3. Wireless Netzwerke

Ein aufkommendes Problem für Unternehmen heutzutage ist das der Mobilität. Mitarbeiter von zuhause oder abgelegenen Standorten, Techniker und leitende Angestellte benötigen tragbare Lösungen, wie z.B. Laptops, Persönliche Digitale Assistenten (PDA) und drahtlosen Zugang zu Netzwerkressourcen. Das IEEE (Institue of Electrical and Electronics Engineers), der als Standardisierungsgremium fungierender Ingenieursverband in den USA, hat eine Norm für die 802.11 Wireless-Spezifikation entworfen, die Standards für drahtlose Datenkommunikation in allen Industriezweigen festlegt. Der heutige Standard ist die 802.11g Spezifikation, während .802.11a und 802.11b bereits veraltete Standards sind. Der 802.11g Standard ist kompatibel mit der älteren Version 802.11b, jedoch nicht mit 802.11a.

Die Spezifikationen 802.11b und 802.11g sind eine Gruppe von Standards, die die drahtlose Kommunikazion und Zugangskontrolle unter dem unlizensierten 2.4GHz Radiofrequenz-Spektrum (802.11a verwendet das 5GHz Spektrum) regeln. Diese Spezifikationen wurden als Standard von IEEE akzeptiert und mehrere Hersteller vermarkten 802.11*x* Produkte und Dienste. Konsumenten haben auch den Standard für kleine Büros/Heimbüros (SOHO) übernommen. Die Beliebtheit hat sich auch von LANs zu MANs (Metropolitan Area Networks) ausgedehnt, insbesondere in dichtbevölkerten Gegenden, wo eine Konzentration von Wireless Access Points (WAPs) zur Verfügung steht. Es gibt desweiteren Wireless Internet Service Provider (WISPs), die sich auf Reisende mit Bedarf an Broadband-Internet Zugang spezialisieren.

Die 802.11*x* Spezifikation ermöglicht direkte, Peer-to-Peer Verbindungen zwischen Knoten durch wireless NICs. Diese lose Gruppe von Knoten, auch *ad hoc* Netzwerk genannt, ist ideal für schnelles Teilen von Verbindungen zwischen zwei oder mehr Knoten, besitzt jedoch Anpassbarkeitsprobleme, die nicht für bestimmte Wireless-Konnektivität geeignet sind.

Eine besser geeignete Lösung für Wireless-Zugang in festen Strukturen ist die Installation einer oder mehrerer WAPs (drahtlose Anwenderprotokolle), die mit dem traditionellen Netzwerk verbunden sind und Wireless-Knoten ermöglichen, sich mit dem WAP zu verbinden, als wenn dies ein Ethernet-Netzwerk wäre. Das WAP handelt hier effektiv als eine Brücke zwischen den Knoten, die mit ihm und dem Rest des Netzwerks verbunden sind.

A.1.3.1. 802.11*x* Sicherheit

Auch wenn Wireless-Netzwerk von Geschwindigkeit und Bequemlichkeit her geeigneter sind als traditionelle Netzwerke, gibt es einige Einschränkungen für die Spezifikationen, die eine genaue Betrachtung erfordern. Die wichtigste Einschränkung ist die Implementierung der Sicherheit.

In der Aufregung eines erfolgreichen Einsatzes eines 802.11*x* Netzwerks, vergessen viele Administratoren selbst die grundlegendsten Sicherheitsmaßnahmen. Da das 802.11*x* Networking über hochfrequente RF-Signale durchgeführt wird, ist dies leicht zugänglich für Benutzer mit einem kompatiblem NIC, einem Wireless-Netzwerk-Scan-Tool wie **NetStumbler** oder **Wellenreiter** und herkömmlichen Sniffing-Tools wie `dsniff` und `snort`. Um einen Missbrauch privater Wireless-Netzwerke zu verhindern, verwendet der 802.11b Standard das Wired Equivalency Privacy (WEP) Protokoll, das ein RC4-basierter 64- oder 128-Bit verschlüsselter Schlüssel ist, der von den Knoten oder zwischen AP und Knoten gemeinsam verwendet wird. Dieser Schlüssel verschlüsselt Übertragungen und entschlüsselt eingehende Pakete dynamisch und transparent. Administratoren denken oft nicht an den Einsatz dieses Shared-Key-Verschlüsselungs-Schematas; entweder weil diese es schlichtweg vergessen oder aufgrund der Leistungsbeeinträchtigung insbseondere über weite Entfernungen. Der Einsatz von WEP für Wireless Netzwerke kann die Wahrscheinlichkeit des Abfangens von Daten wesentlich verringern.

Red Hat Enterprise Linux unterstützt mehrere 802.11*x* Produkte verschiedener Hersteller. Das **Network Administration Tool** beinhaltet eine Möglichkeit für das Konfigurieren von Wireless NICs und WEP-Sicherheit. Weitere Informationen zum **Network Administration Tool** finden Sie im Kapitel *Netzwerk-Konfiguration* im*Red Hat Enterprise Linux Handbuch zur System-Administration*.

Sich auf WEP zu verlassen ist jedoch weiterhin nicht ausreichend zum Schutz vor entschlossenen Angreifern. Es gibt spezialisierte Utilities, die zum Cracken der RC4 WEP Verschlüsselungsalgorithmen, die ein Wireless Netzwerk schützen, entwickelt wurden und die den gemeinsamen Schlüssel

aufdecken. **AirSnort** und **WEP Crack** sind solche Applikationen. Um sich hiervor zu schützen, sollten Administratoren strenge Richtlinien für die Verwendung von Wireless Methoden zum Zugang zu empfindlichen Informationen festlegen. Administratoren können z.B. die Sicherheit der Wireless-Konnektivität erhöhen, in dem diese auf nur VPN- und SSH-Verbindungen beschränkt werden, die eine weitere Verschlüsselungschicht zusätzlich zur WEP-Verschlüsselung bietet. Durch diese Richtlinien muss ein Angreifer außerhalb des Netzwerkes, der die WEP-Verschlüsselung geknackt hat, noch zusätzlich die VPN oder SSH-Verschlüsselung knacken, die abhängig von der Verschlüsselungsmethode bis zu dreifach 168-bit DES Algorithmus-Verschlüsselung (3DES) oder noch stärkere proprietäre Algorithmen enthalten kann. Administratoren, die diese Richtlinien anwenden, sollten Nur-Text-Protokolle wie Telnet oder FTP einschränken, da Passwörter und Daten während der bereits erwähnten Angriffe aufgedeckt werden können.

Eine moderne Sicherheits- und Authentifizierungsmethode, welche von Herstellern von Netzwerkfunkausrüstung eingeführt wurde, ist *Wi-fi Protected Access* (WPA). Administratoren können WPA mit Hilfe eines Authentifizierungsservers auf deren Netzwerk konfigurieren, welcher Keys für Clients verwaltet, die auf das funkbetriebene Netzwerk zugreifen. WPA besitzt einen Vorteil gegenüber WEP -Verschlüsselung durch die Benutzung des *Temporal Key Integrity Protocol* (TKIP), wessen Methodik auf der gemeinsamen Benutzung eines Keys basiert, welcher mit der MAC-Adresse derWireless-Netzwerkkarte verbunden wird, die auf dem jeweiligen Client installiert ist. Der Wert des gemeinsam benutzten Keys und der MAC-Adresse wird sodann von einem *Initialization Vector* (IV) oder Initialisierungs-Vektor verarbeitet, welcher zur Erstellung eines Keys verwendet wird, welcher sodann jedes einzelne Datenpaket verschlüsselt. IV ändert die Verschlüsselung jedes mal, wenn ein Paket transferiert wird, wobei die üblichsten Funknetz-Attacken vermieden werden können.

Jedoch wird WPA unter Benutzung von TKIP als eher temporäre Lösung angesehen. Lösungen, welche stärkere Verschlüsselungsmethoden anwenden (wie z.B. AES) werden derzeit entwickelt und besitzen das Potential, die Funk-Netzwerksicherheit im Unternehmensbereich weitgehend zu verbessern.

Für weitere Informationen über 802.11 siehe folgende URL:

```
http://standards.ieee.org/getieee802/802.11.html
```

A.1.4. Netzwerk-Segemntierung und DMZ

Administratoren, die extern-zugängliche Dienste wie HTTP, E-Mail, FTP und DNS ausführen wollen, wird empfohlen, diese öffentlich zugänglichen Dienste physikalisch und/oder logisch getrennt vom internen Netzwerk zu halten. Firewalls und das Sichern von Hosts und Applikationen sind effektive Methoden mögliche Einbrecher abzuhalten. Entschlossene Cracker können jedoch Wege in das interne Netzwerk finden, wenn sich die gecrackten Dienste auf der gleichen logischen Route wie der Rest des Netzwerks befinden. Die extern zugänglichen Dienste sollten sich in der *De-Militarisierten Zone* (DMZ) befinden, ein logisches Netzwerksegment, bei dem eingehender Verkehr vom Internet auch nur auf diese Dienste und nicht auf das interne Netzwerk zugreifen kann. Dies ist effektiv, da selbst wenn ein Computer oder DMZ von einem Angreifer erforscht wird, der Rest des internen Netzwerkes hinter einer Firewall auf einem separaten Segment liegt.

Da die meisten Unternehmen einen begrenzten Pool an öffentlich weiterleitbaren IP-Adressen haben, von denen aus externe Dienste ausgeführt werden können, verwenden Administratoren ausgeklügelte Firewall-Regeln zum Annehmen, Weiterleiten, Ablehnen und Verweigern von Paketübertragungen. Firewall-Regeln, die mit `iptables` implementiert wurden oder spezielle Hardware-Firewalls ermöglichen komplexe Routing- und Forwarding-Regeln, mit denen Administratoren eingehenden Verkehr an bestimmte Dienste an bestimmten Adressen und Ports segmentieren können. Lediglich dem LAN wird erlaubt, auf interne Dienste zuzugreifen, was wiederum IP-Spoofing verhindert. Weitere Informationen über das Implementieren von `iptables` finden Sie unter Kapitel 7.

A.2. Hardware-Sicherheit

Laut einer im Jahre 2000 vom FBI und CSI (Computer Security Institute) durchgeführten Studie erfolgten über siebzig Prozent aller gemeldeten Angriffe auf empfindliche Daten und Ressourcen von innerhalb des jeweiligen Unternehmens. Das Implementieren einer internen Sicherheits-Police ist daher genauso wichtig wie eine externe Strategie. Dieser Abschnitt erklärt einige der Schritte, die Administratoren und Benutzer zur Sicherung der Systeme vor internen Angriffen durchführen können.

Mitarbeiter-Workstations sind relativ unwahrscheinliche Angriffsziele für aus der Ferne verübte Attacken, insbesondere solche hinter einer gut konfigurierten Firewall. Es können jedoch einige Schutzmaßnahmen implementiert werden, um interne oder physikalische Attacken auf individuelle Workstation-Ressourcen zu verhindern.

Moderne Workstation und Heim-PCs haben BIOSe, die Systemressourcen auf Hardwareebene kontrollieren. Workstation-Benutzer können administrative Passwörter innerhalb des BIOS festlegen, um bösartige Benutzer am Zugriff oder am Booten des Systems zu hindern. BIOS-Passwörter hindern Angreifer amf Booten des Systems und halten diese davon ab, schnell Zugang zu Informationen auf der Festplatte zu erhalten oder zu stehlen.

Stiehlt jedoch der Angreifer den PC (der häufigste Fall von Diebstahl unter Reisenden, die Laptops und andere mobile Geräte mit sich tragen) und bringt diesen zu einem Ort, an dem er den PC auseinandernehmen kann, hält das BIOS-Passwort den Angreifer nichr davon ab, die Festplatte zu entfernen und diese in einem PC ohne BIOS-Einschränkungen einzubauen und somit Zugang zu den Informationen zu erhalten. In diesen Fällen wird empfohlen, dass Workstations abgeschlossen werden, um Zugang zur internen Hardware einzuschränken. Besondere Sicherheitsmaßnahmen wie abschließbare Stahlkabel können an einem PC oder Laptop angebracht werden, um Diebstahl zu verhindern, und darüberhinaus Schlösser am Gehäuse, um internen Zugang zu verhindern. Diese Art Hardware ist nahezu überall von Herstellern wie z.B. Kensington und Targus erhältlich.

Server-Hardware, insbesondere Produktionsserver, sind gewöhnlich auf Regalen in Serverräumen montiert. Server-Schränke haben normalerweise abschließbare Türen und einzelne Servergehäuse sind auch mit abschließbaren Fronten erhältlich, um den Schutz vor unbeabsichtigtem oder beabsichtigtem Herunterfahren zu erhöhen.

Unternehmen können auch sog. Co-Location Anbieter zur Unterbringung derer Server verwenden, da diese höhere Bandbreite, 24/7 Support und Erfahrung in der System- und Serversicherheit besitzen. Dies kann eine effektive Methode zum Auslagern von Sicherheits- und Konnektivitätsanfoderungen für HTTP-Transaktionen oder Streaming Media Services sein. Co-Location kann sich jedoch als sehr kostenintensiv erweisen. Co-Location-Standorte sind bekannt für starke Absicherung durch geschultes Sicherheitspersonal und ständige Überwachung.

Anhang B.

Häufige Schwachstellen und Attacken

Tabelle B-1 zeigt einige der von Eindringlingen am häufigsten ausgenutzten Schwachstellen und Zugangspunkte zum Zugriff auf Netzwerkressourcen in einem Unternehmen. Der Schlüssel zu diesen häufigen Schwachstellen ist die Erklärung, wie diese ausgenutzt werden, und wie Administratoren ihr Netzwerk ordnungsgemäß gegen solche Angriffe schützen können.

Sicherheitsloch	Beschreibung	Hinweise
Null- oder Standardpasswort	Das Leerlassen von Passwörtern oder das Verwenden von bereits bestehenden Standardpasswörtern, die mit einer Applikation mitgeliefert werden. Dies kommt am häufigsten bei Hardware wie Router und BIOS vor; einige Dienste, die unter Linux laufen, können jedoch auch standardmäßige Administratoren-Passwörter enthalten (Red Hat Enterprise Linux wird jedoch nicht mit Solchen ausgeliefert)	Häufig mit Netzwerk-Hardware wie Routers, Firewalls, VPNs und Netzwerkspeicher-Applikationen (NAS) assoziiert. Tritt häufig in Legacy-Betriebssystemen auf, insbesondere bei Betriebssystemen, die Dienste wie UNIX und Windows kombinieren. Administratoren erstellen manchmal berechtigte Benutzer in Eile, und lassen das Passwort frei, ein perfekter Zugangspunkt für bösartige Benutzer, die dies entdecken.
Standard Shared Keys	Sichere Dienste werden manchmal mit standardmäßigen Sicherheitsschlüsseln für Entwicklung oder zu Evaluationszwecken ausgeliefert. Werden diese Schlüssel nicht geändert und in eine Produktionsumgebung im Internet gestellt, kann *jeder* Benutzer mit dem gleichen Standardschlüssel auf diese Ressourcen und damit auf alle empfindlichen Informationen darin zugreifen.	Tritt in Wireless Access Points und bei vorkonfigurierten, sicheren Servern auf. CIPE (siehe Kapitel 6) enthält als Beispiel einen statischen Schlüssel, der geändert werden muss, bevor dieser in einer Produktionsumgebung angewendet wird.

Sicherheitsloch	Beschreibung	Hinweise
IP-Spoofing	Eine sich entfernt befindliche Maschine verhält sich wie ein Knoten im lokalen Netzwerk, findet Schwachstellen auf Ihrem Server und installiert ein Backdoor-Programm oder Trojanisches Pferd, um Kontrolle über Ihre Netzwerkressourcen zu erlangen.	Spoofing ist relativ schwierig, da es vom Angreifer erfordert, dass er TCP/IP SYN-ACK-Nummern voraussagt, um eine Verbindung zum Zielsystem zu koordinieren. Es sind jedoch verschiedene Tools erhältlich, die dem Cracker bei diesem Angriff helfen können. Spoofing ist abhängig von den auf dem System laufenden Dienste (wie `rsh`, `telnet`, FTP und andere), die *Source-basierte* Authentifizierungstechniken verwenden, die im Vergleich zu PKI oder anderen Formen der Verschlüsselung wie `ssh` oder SSL/TLS nicht empfohlen werden.
Lauschen	Das Sammeln von Daten zwischen zwei aktiven Knoten auf einem Netzwerk durch das Abhören der Verbindung dieser beiden Knoten.	Diese Art Angriff funktioniert am besten mit Klartext-Übertragungsprotokollen wie Telnet-, FTP- und HTTP-Übertragungen. Angreifer von außerhalb müssen Zugang zu einem kompromittierten System in einem LAN haben, um solch eine Attacke durchführen zu können; meistens hat der Cracker bereits aktiv eine Attacke ausgeführt (wie z.B. IP-Spoofing oder Man-in-the-Middle). Vorbeugende Maßnahmen umfassen Dienste mit verschlüsseltem Schlüssel-Austausch, einmalige Passwörter oder verschlüsselte Authentifizierung gegen das Erschnüffeln von Passwörtern; verstärkte Verschlüsselung während der Übertragung ist auch angeraten.

Sicherheitsloch	Beschreibung	Hinweise
Schwachstellen von Diensten	Ein Angreifer findet einen Fehler oder ein Schlupfloch in einem Dienst, der über das Internet läuft. Durch diese Anfälligkeit kann der Angreifer das gesamte System und alle Daten darauf sowie weitere Systeme im Netzwerk kompromittieren.	HTTP-basierte Dienste wie CGI sind anfällig für entfernte Befehlsausführungen und sogar interaktiven Zugang zur Shell. Auch wenn der HTTP-Dienst unter einem nicht-privilegierten Benutzer wie "Nobody" ausgeführt wird, können Informationen wie Konfigurationsdateien und Netzwerkpläne gelesen werden. Der Angreifer könnte auch eine Denial-of-Service-Attacke starten, die die Systemressourcen lahmlegt oder für andere Benutzer unzugänglich macht. Dienste weisen manchmal Anfälligkeiten auf, die während der Entwicklung und dem Testen unbemerkt bleiben. Diese Anfälligkeiten sind z.B. *Buffer Overflows*, bei dem Angreifer Zugang erhalten, indem sie den Adress-Speicher mit mehr als vom Dienst akzeptierten Inhalt füllen, den Dienst damit zum Absturz bringen und somit Zugang zu einem interaktiven Befehlsprompt bekommen, von dem aus sie Befehle ausführen können. Dies kann komplette administrative Kontrolle für den Attacker bedeuten. Administratoren sollten sicherstellen, dass Dienste nicht als root ausgeführt werden und wachsam sein, wenn es zu Patches und Errata-Updates von Herstellern oder Sicherheitsorganisationen wie CERT und CVE kommt.

Sicherheitsloch	Beschreibung	Hinweise
Schwachstellen von Applikationen	Angreifer finden Fehler in Desktop- und Workstation-Applikationen wie E-Mail-Clients und können willkürlich Code ausführen, Trojaner für zukünftige Attacken implantieren oder Systeme zum Absturz bringen. Es kann noch größerer Schaden angerichtet werden, wenn die kompromittierte Workstation administrative Berechtigungen für den Rest des Netzwerkes hat.	Workstations und Desktops sind anfälliger für eine Ausbeutung als Server, die von Adminsitratoren verwaltet werden, da die Benutzer keine Erfahrung oder nicht das Wissen zur Verhinderung oder Aufdeckung von Einbrüchen haben. Es ist von oberster Wichtigkeit, Einzelpersonen über die Risiken bei der Installation unberechtigter Software oder beim Öffnen vom E-Mail unbekannter Herkunft zu informieren Es können Schutzeinrichtungen installiert werden, so dass z.B. E-Mail-Software nicht automatisch Anhänge öffnen oder ausführen kann. Zusätzlich dazu kann das automatische Aktualisieren der Workstation-Software über das Red Hat Network oder andere System-Management-Services die Last einer vielschichtigen Sicherheitsimplemetierung ausgleichen.
Denial-of-Service (DoS) Attacken	Angreifer oder Gruppen von Angreifern koordinieren eine Attacke auf ein Netzwerk oder Serverressourcen, bei der unbefugte Pakete an den Zielcomputer gesendet werden (entweder Server, Router oder Workstation). Dies zwingt die Ressource für berechtigte Benutzer unverfügbar zu werden.	Der am häufigsten berichtete DoS-Vorfall trat im Jahr 2000 auf, als mehrere stark besuchte kommerzielle Websites und Websites der Regierung angegriffen wurden, wobei durch eine koordinierte Ping-Flut-Attacke mehrere kompromittierte Systeme mit Breitbandverbindungen unverfügbar gemacht wurden, indem sich diese wie *Zombies*verhielten oder Übertragungsknoten umgeleitet wurden. Quell-Pakete werden allgemein gefälscht (oder umgeleitet), was das Auffinden der wahren Quelle der Attacke schwierig macht. Fortschritte beim Ingress Filtering (IETF rfc2267) mittels `iptables` und Netzwerk-IDS-Technologien wie `snort` helfen Administratoren, DoS-Attacken herauszufinden und zu verhindern.

Tabelle B-1. Häufige Sicherheitslöcher

Anhang C.

Häufige Ports

In der folgenden Tabelle werden die häufigsten Kommunikationsports, die von Services, Daemons und Programmen unter Red Hat Enterprise Linux verwendet werden, aufgelistet. Diese Liste finden Sie auch in der Datei `/etc/services`. Diese offizielle Liste bekannter, registrierter und Dynamischer Ports wie von der Internet Assigned Numbers Authority (IANA) ausgegeben finden Sie unter der folgenden URL:

http://www.iana.org/assignments/port-numbers

Hinweis

Der *Layer*, wenn aufgelistet, besagt, ob der Service oder das Protokoll TCP oder UDP für die Übertragung verwendet. Wenn nicht aufgelistet, verwenden Service/Protokoll beides, TCP und UDP.

Tabelle C-1 listet die von IANA ausgegebenen "Bekannten Ports" auf und wird von Red Hat Enterprise Linux für Standard-Komminukations-Ports für verschiedene Services, inklusive FTP, SSH und Samba verwendet.

Port # / Layer	Name	Kommentar
1	tcpmux	TCP Port Service Multiplexer
5	rje	Jobferneingabe (RJE)
7	echo	Echo-Service
9	discard	Null-Service für das Prüfen von Verbindungen
11	systat	System-Status Service für das Auflisten verbundener Ports
13	daytime	Sendet Datum und Zeit an anfragenden Host
17	qotd	Sendet Zitat des Tages an einen verbundenen Host
18	msp	Message Send Protocol (MSP)
19	chargen	Character Generation Service; sendet endlose Zeichenketten
20	ftp-data	FTP-Datenport
21	ftp	File Transfer Protocol (FTP) Port; manchmal vom File Service Protocol (FSP) verwendet
22	ssh	Secure Shell (SSH) Service
23	telnet	Der Telnet Service
25	smtp	Simple Mail Transfer Protocol (SMTP)
37	time	Time Protocol (Zeitprotokoll)
39	rlp	Resource Location Protocol

Port # / Layer	Name	Kommentar
42	nameserver	Internet Name Service
43	nicname	WHOIS Verzeichnis-Service
49	tacacs	Terminal Access Controller Access Control System für TCP/IP-basierte Authentifizierung und Zugriff
50	re-mail-ck	Remote Mail Checking Protocol
53	domain	Domain Name Services (wie BIND)
63	whois++	WHOIS++, erweiterte WHOIS-Services
67	bootps	Bootstrap Protocol (BOOTP) Services; auch von Dynamic Host Configuration Protocol (DHCP) Services verwendet
68	bootpc	Bootstrap (BOOTP) Client; auch von Dynamic Host Control Protocol (DHCP) Clients verwendet
69	tftp	Trivial File Transfer Protocol (TFTP)
70	gopher	Gopher Internet Dokumentsuche und -auffindung
71	netrjs-1	Remote Job Service
72	netrjs-2	Remote Job Service
73	netrjs-3	Remote Job Service
73	netrjs-4	Remote Job Service
79	finger	Finger Service für Benutzer-Kontaktinformationen
80	http	HyperText Transfer Protocol (HTTP) für World Wide Web (WWW) Services
88	kerberos	Kerberos Netzwerk-Authentifizierungssystem
95	supdup	Telnet Protokoll-Erweiterung
101	hostname	Hostname Services auf SRI-NIC Computern
102/tcp	iso-tsap	ISO Development Environment (ISODE) Netzwerk-Applikationen
105	csnet-ns	Mailbox Nameserver; auch von CSO Nameserver verwendet
107	rtelnet	Remote Telnet
109	pop2	Post Office Protocol Version 2
110	pop3	Post Office Protocol Version 3
111	sunrpc	Remote Procedure Call (RPC) Protokoll für Remote-Befehlsausführung, verwendet vom Network Filesystem (NFS)
113	auth	Authentication und Ident Protokolle
115	sftp	Secure File Transfer Protocol (SFTP) Services
117	uucp-path	Unix-to-Unix Copy Protocol (UUCP) Path Services
119	nntp	Network News Transfer Protocol (NNTP) für das USENET Discussion System

Port # / Layer	Name	Kommentar
123	ntp	Network Time Protocol (NTP)
137	netbios-ns	NETBIOS Name Service unter Red Hat Enterprise Linux von Samba verwendet
138	netbios-dgm	NETBIOS Datagram Service unter Red Hat Enterprise Linux von Samba verwendet
139	netbios-ssn	NETBIOS Session Service unter Red Hat Enterprise Linux von Samba verwendet
143	imap	Internet Message Access Protocol (IMAP)
161	snmp	Simple Network Management Protocol (SNMP)
162	snmptrap	Traps für SNMP
163	cmip-man	Common Management Information Protocol (CMIP)
164	cmip-agent	Common Management Information Protocol (CMIP)
174	mailq	MAILQ Email Transport Queue
177	xdmcp	X Display Manager Control Protocol (XDMCP)
178	nextstep	NeXTStep Window Server
179	bgp	Border Gateway Protocol
191	prospero	Prospero distributed Filesystem Services
194	irc	Internet Relay Chat (IRC)
199	smux	SNMP UNIX Multiplexer
201	at-rtmp	AppleTalk Routing
202	at-nbp	AppleTalk Name Binding
204	at-echo	AppleTalk Echo
206	at-zis	AppleTalk Zone Information
209	qmtp	Quick Mail Transfer Protocol (QMTP)
210	z39.50	NISO Z39.50 Database
213	ipx	Internetwork Packet Exchange (IPX), ein Datagram Protokoll, das häufig in Novell Netware Umgebungen verwendet wird
220	imap3	Internet Message Access Protocol Version 3
245	link	LINK / 3-DNS iQuery Service
347	fatserv	FATMEN File and Tape Management Server
363	rsvp_tunnel	RSVP Tunnel
369	rpc2portmap	Coda Filesystem Portmapper
370	codaauth2	Coda File System Authentication Services
372	ulistproc	UNIX LISTSERV
389	ldap	Lightweight Directory Access Protocol (LDAP)
427	svrloc	Service Location Protocol (SLP)

Port # / Layer	Name	Kommentar
434	mobileip-agent	Mobile Internet Protocol (IP) Agent
435	mobilip-mn	Mobile Internet Protocol (IP) Manager
443	https	Secure Hypertext Transfer Protocol (HTTP)
444	snpp	Simple Network Paging Protocol
445	microsoft-ds	Server Message Block (SMB) über TCP/IP
464	kpasswd	Kerberos Passwort und Schlüsse-Änderungs-Service
468	photuris	Photuris Session Key Management Protokoll
487	saft	Simple Asynchronous File Transfer (SAFT) Protokoll
488	gss-http	Generic Security Services (GSS) für HTTP
496	pim-rp-disc	Rendezvous Point Discovery (RP-DISC) für Protocol Independent Multicast (PIM) Services
500	isakmp	Internet Security Association und Key Management Protocol (ISAKMP)
535	iiop	Internet Inter-Orb Protocol (IIOP)
538	gdomap	GNUstep Distributed Objects Mapper (GDOMAP)
546	dhcpv6-client	Dynamic Host Configuration Protocol (DHCP) Version 6 Client
547	dhcpv6-server	Dynamic Host Configuration Protocol (DHCP) Version 6 Service
554	rtsp	Real Time Stream Control Protocol (RTSP)
563	nntps	Network News Transport Protocol über Secure Sockets Layer (NNTPS)
565	whoami	Whoami User ID Listing
587	submission	Mail Message Submission Agent (MSA)
610	npmp-local	Network Peripheral Management Protocol (NPMP) local / Distributed Queueing System (DQS)
611	npmp-gui	Network Peripheral Management Protocol (NPMP) GUI / Distributed Queueing System (DQS)
612	hmmp-ind	HyperMedia Management Protocol (HMMP) Indication / DQS
631	ipp	Internet Printing Protocol (IPP)
636	ldaps	Lightweight Directory Access Protocol über Secure Sockets Layer (LDAPS)
674	acap	Application Configuration Access Protocol (ACAP)
694	ha-cluster	Heartbeat Services für High-Availability Clusters
749	kerberos-adm	Kerberos Version 5 (v5) 'kadmin' Datenbankverwaltung
750	kerberos-iv	Kerberos Version 4 (v4) Services
765	webster	Network Dictionary

Port # / Layer	Name	Kommentar
767	phonebook	Network Phonebook
873	rsync	rsync Dateitransfer-Services
992	telnets	Telnet über Secure Sockets Layer (TelnetS)
993	imaps	Internet Message Access Protocol über Secure Sockets Layer (IMAPS)
994	ircs	Internet Relay Chat über Secure Sockets Layer (IRCS)
995	pop3s	Post Office Protocol Version 3 über Secure Sockets Layer (POP3S)

Tabelle C-1. Bekannte Ports

Tabelle C-2 listet UNIX-spezifische Ports und Cover-Services, von Email bis hin zur Authentifizierung und vieles mehr. Namen in Klammern (z.B. [*service*]) sind entweder Daemon-Namen für den Service oder bekannte Aliase.

Port # / Layer	Name	Kommentar
512/tcp	exec	Authentifizierung für Remote-Prozess-Ausführung
512/udp	biff [comsat]	Asynchrous Mail Client (biff) und Service (comsat)
513/tcp	login	Remote Login (rlogin)
513/udp	who [whod]	Whod User Logging Daemon
514/tcp	shell [cmd]	Remote Shell (rshell) und Remote Copy (rcp) ohne Logging
514/udp	syslog	UNIX System-Logging Service
515	printer [spooler]	Line Printer (lpr) Spooler
517/udp	talk	Talk Remote Calling-Service und Client
518/udp	ntalk	Network talk (ntalk) Remote Calling Service und Client
519	utime [unixtime]	UNIX (utime) Zeitprotokoll
520/tcp	efs	Extended Filename Server (EFS)
520/udp	router [route, routed]	Routing Information Protocol (RIP)
521	ripng	Routing Information Protocol für Internet Protocol Version 6 (IPv6)
525	timed [timeserver]	Time Daemon (timed)
526/tcp	tempo [newdate]	Tempo
530/tcp	courier [rpc]	Courier Remote Procedure Call (RPC) Protokoll
531/tcp	conference [chat]	Internet Relay Chat
532	netnews	Netnews Newsgroup Service
533/udp	netwall	Netwall für Notfall-Broadcasts

Port # / Layer	Name	Kommentar
540/tcp	uucp [uucpd]	UNIX-to-UNIX Copy Services
543/tcp	klogin	Kerberos Version 5 (v5) Remote Login
544/tcp	kshell	Kerberos Version 5 (v5) Remote Shell
548	afpovertcp	Appletalk Filing Protocol (AFP) über Transmission Control Protocol (TCP)
556	remotefs [rfs_server, rfs]	Brunhoff's Remote Filesystem (RFS)

Tabelle C-2. UNIX-spezifische Ports

Tabelle C-3 listet Ports, die von der Netzwerk- und Software-Community an die IANA für formelle Registrierung in der Portnummernliste weitergegeben wurden.

Port # / Layer	Name	Kommentar
1080	socks	SOCKS Netzwerk-Applikations Proxy-Services
1236	bvcontrol [rmtcfg]	Remote-Konfigurationsserver für Gracilis Packeten Netzwerk-Switche[a]
1300	h323hostcallsc	H.323 Telecommunication Host Call Secure
1433	ms-sql-s	Microsoft SQL Server
1434	ms-sql-m	Microsoft SQL Monitor
1494	ica	Citrix ICA Client
1512	wins	Microsoft Windows Internet Name Server
1524	ingreslock	Ingres Database Management System (DBMS) Lock Services
1525	prospero-np	Prospero Non-Priveleged
1645	datametrics [old-radius]	Datametrics / old radius entry
1646	sa-msg-port [oldradacct]	sa-msg-port / old radacct entry
1649	kermit	Kermit Dateitransfer und Management Service
1701	l2tp [l2f]	Layer 2 Tunneling Protocol (LT2P) / Layer 2 Forwarding (L2F)
1718	h323gatedisc	H.323 Zelecommunication Gatekeeper Discovery
1719	h323gatestat	H.323 Telecommunication Gatekeeper Status
1720	h323hostcall	H.323 Telecommunication Host Call setup
1758	tftp-mcast	Trivial FTP Multicast
1759/udp	mtftp	Multicast Trivial FTP (MTFTP)
1789	hello	Hello Router Kommunikationsprotokoll
1812	radius	Radius Dial-up Authentifizierungs- und Accounting-Service

Port # / Layer	Name	Kommentar
1813	radius-acct	Radius Accounting
1911	mtp	Starlight Networks Multimedia Transport Protocol (MTP)
1985	hsrp	Cisco Hot Standby Router Protokoll
1986	licensedaemon	Cisco License Management Daemon
1997	gdp-port	Cisco Gateway Discovery Protocol (GDP)
2049	nfs [nfsd]	Network File System (NFS)
2102	zephyr-srv	Zephyr distributed Messaging Server
2103	zephyr-clt	Zephyr Client
2104	zephyr-hm	Zephyr Host Manager
2401	cvspserver	Concurrent Versions System (CVS) Client/Server Operations
2430/tcp	venus	Venus Cache Manager für Coda Dateisystem (codacon port)
2430/udp	venus	Venus Cache Manager für Coda Dateisystem (callback/wbc interface)
2431/tcp	venus-se	Venus Transmission Control Protocol (TCP) Nebeneffekte
2431/udp	venus-se	Venus User Datagram Protocol (UDP) Nebeneffekte
2432/udp	codasrv	Coda Dateisystem Server Port
2433/tcp	codasrv-se	Coda Dateisysten TCP Nebeneffekte
2433/udp	codasrv-se	Coda Dateisysten UDP SFTP Nebeneffekte
2600	hpstgmgr [zebrasrv]	Zebra Routing[b]
2601	discp-client [zebra]	discp client; Zebra Integrated Shell
2602	discp-server [ripd]	discp server; Routing Information Protocol Daemon (ripd)
2603	servicemeter [ripngd]	Service Meter; RIP Daemon für IPv6
2604	nsc-ccs [ospfd]	NSC CCS; Open Shortest Path First Daemon (ospfd)
2605	nsc-posa	NSC POSA; Border Gateway Protocol Daemon (bgpd)
2606	netmon [ospf6d]	Dell Netmon; OSPF für IPv6 Daemon (ospf6d)
2809	corbaloc	Common Object Request Broker Architecture (CORBA) Naming Service Locator
3130	icpv2	Internet Cache Protocol Version 2 (v2); verwendet vom Squid Proxy Caching Server
3306	mysql	MySQL Datenbank Service
3346	trnsprntproxy	Transparent Proxy

Port # / Layer	Name	Kommentar
4011	pxe	Pre-execution Environment (PXE) Service
4321	rwhois	Remote Whois (rwhois) Service
4444	krb524	Kerberos Version 5 (v5) to Version 4 (v4) Ticket Translator
5002	rfe	Radio Free Ethernet (RFE) Audio Broadcasting System
5308	cfengine	Configuration Engine (Cfengine)
5999	cvsup [CVSup]	CVSup Dateitransfer und Update-Tool
6000/tcp	x11 [X]	X Window System Services
7000	afs3-fileserver	Andrew File System (AFS) Dateiserver
7001	afs3-callback	AFS Port für Callbacks to Cache Manager
7002	afs3-prserver	AFS Benutzer- und Gruppendatenbank
7003	afs3-vlserver	AFS Volume Location Datenbank
7004	afs3-kaserver	AFS Kerberos Authentifizierungsservice
7005	afs3-volser	AFS Volume Management Server
7006	afs3-errors	AFS Fehler-Interpretationsservice
7007	afs3-bos	AFS Basic Overseer Process
7008	afs3-update	AFS Server-to-Server Updater
7009	afs3-rmtsys	AFS Remote Cache Manager Service
9876	sd	Session Director für IP Multicast Conferencing
10080	amanda	Advanced Maryland Automatic Network Disk Archiver (Amanda) Backup Services
11371	pgpkeyserver	Pretty Good Privacy (PGP) / GNU Privacy Guard (GPG) Public Keyserver
11720	h323callsigalt	H.323 Call Signal Alternate
13720	bprd	Veritas NetBackup Request Daemon (bprd)
13721	bpdbm	Veritas NetBackup Database Manager (bpdbm)
13722	bpjava-msvc	Veritas NetBackup Java / Microsoft Visual C++ (MSVC) Protocol
13724	vnetd	Veritas Network Utility
13782	bpcd	Veritas NetBackup
13783	vopied	Veritas VOPIE Authentication Daemon
22273	wnn6 [wnn4]	Kana/Kanji Konvertierungssystem$_c$
26000	quake	Quake (und andere) Multi-Player Spieleserver
26208	wnn6-ds	Wnn6 Kana/Kanji Server
33434	traceroute	Traceroute Netzwerk-Tracking-Tool

Port # / Layer	Name	Kommentar
Bemerkungen: a. Hinweis in `/etc/services`: "Port 1236 ist registriert als 'bvcontrol', wird jedoch auch von Gracilis Packeten Remote Config Server verwendet. Der offizielle Name ist als Hauptname gelistet, der unregistrierte Name wird als Alias geführt." b. Hinweis in `/etc/services`: "Ports mit der Nummer 2600 bis 2606 werden vom Zebra-Paket ohne Registrierung verwendet. Die Hauptnamen sind die registrierten Namen, und die von zebra verwendeten unregistrierten Namen werden als Alias gelistet." c. Hinweis in `/etc/services`: "Dieser Port ist unter wnn6 registriert, jedoch auch unter dem unregistrierten Namen 'wnn4' vom FreeWnn Paket."		

Tabelle C-3. Registrierte Ports

Tabelle C-4 zeigt eine Liste der Ports, die sich auf das Datagram Delivery Protocol (DDP) auf AppleTalk Netzwerken beziehen.

Port # / Layer	Name	Kommentar
1/ddp	rtmp	Routing Table Management Protocol
2/ddp	nbp	Name Binding Protocol
4/ddp	echo	AppleTalk Echo Protocol
6/ddp	zip	Zone Information Protocol

Tabelle C-4. Datagram Deliver Protocol Ports

Tabelle C-5 ist eine Liste von Ports, die sich auf das Kerberos Netzwerk-Authentifizierungsprotokoll beziehen. Wenn angegeben bezieht sich v5 auf das Kerberos Version 5 Protokoll. Beachten Sie bitte, dass diese Ports nicht bei der IANA registriert sind.

Port # / Layer	Name	Kommentar
751	kerberos_master	Kerberos Authentifizierung
752	passwd_server	Kerberos Password (kpasswd) Server
754	krb5_prop	Kerberos v5 Slave Propagation
760	krbupdate [kreg]	Kerberos Registrierung
1109	kpop	Kerberos Post Office Protocol (KPOP)
2053	knetd	Kerberos De-Multiplexor
2105	eklogin	Kerberos v5 Verschlüsselter Remote-Login (rlogin)

Tabelle C-5. Kerberos (Project Athena/MIT) Ports

Tabelle C-6 ist eine Liste unregistrierter Ports, die von Services und Protokollen, die auf Ihrem Red Hat Enterprise Linux-System installiert sind, verwendet werden oder die notwendig für die Kommunikation zwischen Red Hat Enterprise Linux und anderen Betriebssystemen sind.

Port # / Layer	Name	Kommentar
15/tcp	netstat	Network Status (netstat)
98/tcp	linuxconf	Linuxconf Linux AdministrationS-Tool

Port # / Layer	Name	Kommentar
106	poppassd	Post Office Protocol Password Change Daemon (POPPASSD)
465/tcp	smtps	Simple Mail Transfer Protocol over Secure Sockets Layer (SMTPS)
616/tcp	gii	Gated (routing daemon) Interactive Interface
808	omirr [omirrd]	Online Mirror (Omirr) Datei Mirroring Services
871/tcp	supfileserv	Software Upgrade Protocol (SUP) Server
901/tcp	swat	Samba Web Administration Tool (SWAT)
953	rndc	Berkeley Internet Name Domain Version 9 (BIND 9) Remote Configuration Tool
1127/tcp	supfiledbg	Software Upgrade Protocol (SUP) Debugging
1178/tcp	skkserv	Simple Kana to Kanji (SKK) Japanese Input Server
1313/tcp	xtel	Französisches Minitel Textinformations-System
1529/tcp	support [prmsd, gnatsd]	GNATS Bug Tracking System
2003/tcp	cfinger	GNU Finger
2150	ninstall	Network Installation Service
2988	afbackup	afbackup Client-Server Backup System
3128/tcp	squid	Squid Web Proxy Cache
3455	prsvp	RSVP port
5432	postgres	PostgreSQL Datenbank
4557/tcp	fax	FAX Übertragungs-Service (alter Service)
4559/tcp	hylafax	HylaFAX Client-Server Protokoll (neuer Service)
5232	sgi-dgl	SGI Distributed Graphics Library
5354	noclog	NOCOL Network Operation Center Logging Daemon (noclogd)
5355	hostmon	NOCOL Network Operation Center Host Monitoring
5680/tcp	canna	Canna Japanese Zeigeneingabe-Interface
6010/tcp	x11-ssh-offset	Secure Shell (SSH) X11 Forwarding Offset
6667	ircd	Internet Relay Chat Daemon (ircd)
7100/tcp	xfs	X Font Server (XFS)
7666/tcp	tircproxy	Tircproxy IRC Proxy Service
8008	http-alt	Hypertext Tranfer Protocol (HTTP) Alternate
8080	webcache	World Wide Web (WWW) Caching Service
8081	tproxy	Transparent Proxy
9100/tcp	jetdirect [laserjet, hplj]	Hewlett-Packard (HP) JetDirect Netzwerk-Druck-Service

Port # / Layer	Name	Kommentar
9359	mandelspawn [mandelbrot]	Parallel Mandelbrot Spawning-Programm für das X Window System
10081	kamanda	Amanda Backup Service über Kerberos
10082/tcp	amandaidx	Amanda Index Server
10083/tcp	amidxtape	Amanda Tape Server
20011	isdnlog	Integrated Services Digital Network (ISDN) Logging System
20012	vboxd	ISDN Voice Box Daemon (vboxd)
22305/tcp	wnn4_Kr	kWnn Koreanisch Eingabesystem
22289/tcp	wnn4_Cn	cWnn Chinesisch Eingabesystem
22321/tcp	wnn4_Tw	tWnn Chinesisch Eingabesystem (Taiwan)
24554	binkp	Binkley TCP/IP Fidonet Mailer Daemon
27374	asp	Address Search Protocol
60177	tfido	Ifmail FidoNet kompatibler Mailer Service
60179	fido	FidoNet Elektronische Mail und News Netzwerk

Tabelle C-6. Unregistrierte Ports

Stichwortverzeichnis

Symbole

802.11x, 105
  und Sicherheit, 105
Überblick, 1
Überblick über Sicherheit, 1
  Definition von Computersicherheit, 1
  Denial of Service (DoS), 4
  Entwicklung von Computersicherheit, 1
  Fazit, 7
  Kontrollen
    (Siehe Kontrollen)
  Viren, 4

A

Abonnement-Registrierung, v
Aktivieren Ihres Abonnements, v
Angreifer und Schwachstellen, 9
Apache HTTP Server
  cgi-Sicherheit, 51
  Direktiven, 51
  Einführung, 51

B

Basic Input Output System
  (Siehe BIOS)
Beweise sammeln
    (Siehe Vorfallsreaktion)
  Datei-Prüf-Tools, 96
    dd, 96
    file, 96
    find, 96
    grep, 96
    md5sum, 96
    script, 95
    stat, 96
    strings, 96
BIOS
  nicht-x86-Äquivalente
    Passwörter, 24
  Sicherheit, 23
    Passwörter, 24
Black Hat Hacker
  (Siehe Cracker)
Bootloader
  GRUB
    Passwortschutz, 25
  Sicherheit, 24

C

Co-location Dienste, 107
Computer Emergency Response Team, 94
Cracker
  Black Hat Hacker, 9
  Definition, 9
cupsd, 38

D

Datei-Prüfung
  Tools, 96
dd
  Beweise sammeln mit, 96
  Datei-Prüfung mit, 96
Demilitarisierte Zone, 73
Den Vorfall melden, 99
Denial of Service (DoS)
  Distributed, 4
Dienste, 55
DMZ
  (Siehe Demilitarisierte Zone)
  (Siehe networks)

E

EFI Shell
  Sicherheit
    Passwörter, 24
Einführung, i
  Andere Red Hat Enterprise Linux Handbücher, i
  Kategorien, Verwendung dieses Handbuchs, i
  Themen, i

F

file
  Datei-Prüfung mit, 96
find
  Datei-Prüfung mit, 96
Firewall-Typen, 67
  Network Address Translation (NAT), 67
  Paketfilter, 67
  Proxy, 67
Firewalls, 67
  iptables, 68
  persönliche, 40
  Richtlinien, 70
  stateful , 74
  Typen, 67
  und dynamische (reflexive) Paketfilterung , 74
  und Viruse, 73
  Zusätzliche Informationsquellen, 75
FTP

Anonymer Zugang, 53
anonymes Hochladen, 53
Benutzeraccounts, 54
Einführung, 52
Grußbanner, 52
TCP Wrapper und, 54
vsftpd, 52

G

grep
Datei-Prüfung mit, 96
Grey Hat Hacker
(Siehe Hacker)

H

Hacker
Black Hat
(Siehe Cracker)
Definition, 9
Grey Hat, 9
White Hat, 9
Hacker-Ethik, 9
Hardware, 103
Laptops, 107
Server, 107
und Sicherheit, 107
Workstations, 107
Häufige Ports
Tabelle, 113
Häufige Schwachstellen und Attacken, 109
Tabelle, 109

I

IDS
(Siehe Intrusion Detection Systeme)
Intrusion Detection Systeme, 87
definieren, 87
Host-basiert, 88
netzwerk-basiert, 90
Snort, 92
RPM Paket Manager (RPM), 88
Tripwire, 88
Typen, 87
und Log-Dateien, 88
ip6tables, 74
IPsec, 58
Host-zu-Host, 59
Installieren, 58
Konfiguration, 62
Host-zu-Host, 59
Netzwerk-zu-Netzwerk, 62
Phasen, 58
iptables, 68
Dynamische Paketfilterung, 74
Zustände, 74
Ketten, 69
AUSGABE, 70
EINGABE, 70
FORWARD, 71
POSTROUTING, 72
PREROUTING, 72, 73
Regeln, 70
allgemein, 70
NAT, 72, 73
Speichern, 70
Weiterleitung, 71
Wiederherstellung, 70
Richtlinien, 70
und DMZs, 73
und Viruse, 73
Verwendung von, 69
Zustandsüberprüfung, 74
Zustände, 74
Zusätzliche Informationsquellen, 75

K

Kerberos
NIS, 49
Kommunikationsports, 113
Kommunikationstools
Sicher, 40
GPG, 40
OpenSSH, 40
Kontrollen, 6
administrative, 6
technische, 6
Zugang, 6
Konventionen
Dokument, ii

L

lpd, 38
lsof, 55

M

md5sum
Datei-Prüfung mit, 96

N

NAT
(Siehe Network Address Translation (NAT))
Nessus, 82
Netfilter, 68
Zusätzliche Informationsquellen, 75
Netfilter 6, 74
netstat, 55
Network Address Translation (NAT), 71
mit iptables, 71
Netzwerkdienste, 37
Buffer Overflow
ExecShield, 37
Identifizieren und Konfigurieren, 38
Risiken, 37
Buffer Overflow, 37
Denial-of-Service, 37
Skript-Anfälligkeiten, 37
Netzwerke, 103
de-Militarisierte Zonen (DMZ), 106
Hubs, 104
Segemtierung, 106
Switches, 104
und Sicherheit, 103
Wireless, 105
Netzwerktopologien, 103
Linearer Bus, 103
Ring, 103
Stern, 103
NFS, 49
Netzwerkdesign, 50
Syntax-Fehler, 50
und Sendmail, 55
Nikto, 83
NIS
Einführung, 47
IPTables, 49
Kerberos, 49
Netzwerke planen, 48
NIS-Domain-Name, 48
securenets, 48
Statische Ports, 49
nmap, 55, 82
Befehlszeilenversion, 82

O

OpenSSH, 40
scp, 40
sftp, 40
ssh, 40

P

Password Aging, 30
Passwortsicherheit, 26
aging, 30
Durchsetzung, 29
in einem Unternehmen, 28
Methodologie, 28
Revisionstools, 29
Crack, 29
John the Ripper, 29
Slurpie, 29
sichere Passwörter, 26
und PAM, 29
Passwörter
in einem Unternehmen, 28
Pluggable Authentication Modules (PAM)
Durchsetzung sicherer Passwörter, 29
portmap, 38
und IPTables, 47
und TCP Wrapper, 46
Ports
häufig, 113
Überwachen, 55
Post-Mortem, 95

R

rechtliche Angelegenheiten, 94
Registrieren Ihres Abonnements, v
Risiken
Netzwerke, 10
Architekturen, 10
Offene Ports, 10
Patches und Errata, 11
Server, 10
Unaufmerksame Administration, 11
unsichere Dienste, 12
Workstations und PCs, 12, 12
Applikationen, 12
root, 31
Methoden, 32
mit PAM, 34
SSH-Anmeldungen deaktivieren, 34
Ändern der root-Shell, 33
Zugang beschränken, 34
mit User Manager, 35
und su, 34
und sudo, 36
Zugang erlauben, 31
Zugang sperren, 31
root-Benutzer
(Siehe root)
RPM
GPG-Schlüssel importieren, 18
signierte Pakete verifizieren, 18, 19

und Intrusion Detection, 88

S

Schwachstellen
Analyse, 79
Definition, 80
Entwickeln einer Methode, 81
Test, 80
Analyse mit VLAD the Scanner, 83
mit Nessus bewerten, 82
mit Nikto bewerten, 83
mit Nmap bewerten, 82
sendmail, 38
DoS einschränken, 54
Einführung, 54
und NFS, 55
Server-Sicherheit
Apache HTTP Server, 51
cgi-Sicherheit, 51
Direktiven, 51
FTP, 52
Anonymer Zugang, 53
anonymes Hochladen, 53
Benutzeraccounts, 54
Grußbanner, 52
TCP Wrapper und, 54
vsftpd, 52
NFS, 49
Netzwerkdesign, 50
Syntax-Fehler, 50
NIS, 47
IPTables, 49
Kerberos, 49
Netzwerke planen, 48
NIS-Domain-Name, 48
securenets, 48
Statische Ports, 49
portmap, 46
Ports
Überwachen, 55
Sendmail, 54
DoS einschränken, 54
und NFS, 55
TCP Wrapper, 43
Angriffswarnungen, 44
Banner, 44
Logging, 45
xinetd, 45
DoS verhindern mit, 46
Ressourcen verwalten mit, 46
SENSOR-Falle, 45
Überblick über, 43
Services Configuration Tool, 38
Sicherheits-Errata, 17
Anwenden der Änderungen, 20
via Red Hat Errata-Webseite, 18
wann neu starten, 20
über Red Hat Network, 17
Sicherheitsbetrachtungen
Hardware, 103
Netzwerkübertragung, 104
Physische Netzwerke, 103
Wireless, 105
Snort, 92
sshd, 38
stat
Datei-Prüfung mit, 96
strings
Datei-Prüfung mit, 96
su
und root, 34
sudo
und root, 36

T

TCP Wrapper
Angriffswarnungen, 44
Banner, 44
Logging, 45
und FTP, 54
und portmap, 46
Tripwire, 88

U

Unsichere Dienste, 39
rsh, 39
Telnet, 39
vsftpd, 39
Updates
(Siehe Sicherheits-Errata)

V

Viren
  Trojaner, 4
Virtuelle Private Netzwerke, 57
  IPsec, 58
    Host-zu-Host, 59
    Installieren, 58
    Konfiguration, 62
VLAD Scanner, 83
Vorfallsreaktion
  Beweise sammeln
    Verwenden von dd, 96
  Computer Emergency Response Team (CERT), 94
  Definition von, 93
  Den Vorfall melden, 99
  einen Plan erstellen, 93
  Einführung, 93
  Implementierung, 95
  Informationen nach einem Verstoß sammeln, 96
  Post-Mortem, 95
  und rechtliche Angelegenheiten, 94
  Untersuchung, 95
  Wiederherstellen von Ressourcen, 98
Vorfallsreaktionsplan, 93
VPN, 57

W

White Hat Hacker
  (Siehe Hacker)
Wi-Fi Netzwerke
  (Siehe 802.11x)
Wiederherstellen von Ressourcen, 98
  Das System mit einem Patch versehen, 99
  Neuinstallieren des Systems, 99
Wireless Sicherheit, 105
  802.11x, 105
Workstation-Sicherheit, 23
  Auswertung
    Administrative Kontrolle, 23
    BIOS, 23
    Bootloader, 23
    Kommunikation, 23
    Passwörter, 23
    Persönliche Firewalls, 23
  BIOS, 23
  Bootloader
    Passwörter, 24

X

xinetd, 38
  DoS verhindern mit, 46
  Ressourcen verwalten mit, 46
  SENSOR-Falle, 45

Colophon

Die Handbücher wurden im Format DocBook SGML v4.1 erstellt. Die HTML- und PDF-Formate werden unter Verwendung benutzerdefinierter DSSSL Stylesheets und benutzerdefinierten Jade Wrapper Scripts angelegt. Die DocBook SGML-Dateien wurden in **Emacs** mithilfe von PSGML Mode geschrieben.

Garrett LeSage schuf das Design der Grafiken für Meldungen (Anmerkung, Tipp, Wichtig, Achtung und Warnung). Diese dürfen frei zusammen mit der Red Hat-Dokumentation vertrieben werden.

Das Team der Red Hat-Produktdokumentation besteht aus:

Sandra A. Moore — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™, AMD64 und Intel® Extended Memory 64 Technology (Intel® EM64T)* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® S/390® und IBM® eServer™ zSeries® Architekturen* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® POWER Architecture Architekturen*

John Ha — Verantwortlicher Autor/Bearbeiter des *Red Hat Cluster Suite Configuring and Managing a Cluster*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Bearbeiter von custom DocBook-Stylesheets und Skripts

Edward C. Bailey — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Einführung in die System-Administration*; Verantwortlicher Autor/Bearbeiter der *Release Notes*; Co-Autor des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™, AMD64 und Intel® Extended Memory 64 Technology (Intel® EM64T)*

Karsten Wade — Verantwortlicher Autor/Bearbeiter des *Red Hat SELinux Application Development Guide*; Verantwortlicher Autor/Bearbeiter des *Red Hat SELinux Policy Writing Guide*

Andrius Benokraitis — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Referenzhandbuch*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Handbuch zur System-Administration*

Paul Kennedy — Verantwortlicher Autor/Bearbeiter des *Red Hat GFS Administrator's Guide*; Co-Autor des *Red Hat Cluster Suite Configuring and Managing a Cluster*

Mark Johnson — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Desktop Configuration and Administration Guide*

Melissa Goldin — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Schrittweise Einführung*

Das Red Hat-Team verantwortlich für Übersetzungen besteht aus:

Amanpreet Singh Alam — Technische Übersetzung - Punjabi

Jean-Paul Aubry — Technische Übersetzung - Französisch

David Barzilay — Technische Übersetzung - Portugiesisch (Brasilien)

Runa Bhattacharjee — Technische Übersetzung - Bengali

Chester Cheng — Technische Übersetzung - Traditionelles Chinesisch

Verena Fuehrer — Technische Übersetzung - Deutsch

Kiyoto Hashida — Technische Übersetzung - Japanisch

N. Jayaradha — Technische Übersetzung - Tamil

Michelle Jiyeen Kim — Technische Übersetzung - Koreanisch

Yelitza Louze — Technische Übersetzung - Spanisch

Noriko Mizumoto — Technische Übersetzung - Japanisch

Ankitkumar Rameshchandra Patel — Technische Übersetzung - Gujarati

Rajesh Ranjan — Technische Übersetzung - Hindi
Nadine Richter — Technische Übersetzung - Deutsch
Audrey Simons — Technische Übersetzung - Französisch
Francesco Valente — Technische Übersetzung - Italienisch
Sarah Wang — Technische Übersetzung - Vereinfachtes Chinesisch
Ben Hung-Pin Wu — Technische Übersetzung - Traditionelles Chinesisch